State Federation of Tax Administrators – Enterprise Risk Management (ERM) Workshop

June 24, 2019

Enterprise Risk Management

Chief Risk Officer (CRO)

WA Department of Revenue

Enterprise Risk Officer

State FTA Enterprise Risk Management Workshop Overview

Purpose:

- To provide a general understanding of Enterprise Risk Management.
- Explore two existing ERM programs at tax administrations – one federal and one state – to highlight the benefits experienced as a result of ERM.
- Provide state tax administrators with example ERM program capability and maturity models that can be leveraged to assist with initiating and/or advancing ERM efforts.
- Discuss the top risks faced by state tax administrations (including existing responses and potential impact of risk manifestation).

Expected Outcomes:

- An increased understanding of the purpose and use of ERM.
- Knowledge of ERM activities at the state and federal level that can be leveraged to initiate and/or advance ERM at state tax administrations.
- Increased understanding and awareness of some top risks faced by state tax administrations and activities underway to respond to these risks at certain state tax administrations.

State FTA Enterprise Risk Management Workshop Agenda

Activity	Time
Welcome, Introductions, & Opening Remarks	1:30 PM – 1:35 PM
Overview of Enterprise Risk Management	1:35 PM – 1:40 PM
ERM at the Internal Revenue Service (IRS) ▪ ERM Value Realized ▪ IRS Capability Model ▪ IRS Enterprise Risk List	1:40 PM – 2:15 PM
ERM at Washington State Department of Revenue (DOR) ▪ Washington State DOR Maturity Model ▪ Washington State Enterprise Risk Register	2:15 PM – 2:45 PM
Risks to Tax Administration from a Global Perspective	2:45 PM – 2:55 PM
Introduction to Small Group Activity	2:55 PM – 3:00 PM
Break	3:00 PM – 3:30 PM
Small Group Session: Discussion on Top Risks Facing Tax Administrations	3:30 PM – 4:20 PM
Report out Results from Group Activity	4:20 PM – 4:55 PM
Closing Remarks	4:55 PM – 5:00 PM

Introductions and Opening Remarks

Tom Brandt, IRS, Chief Risk Officer

Tom Brandt has served as the IRS's Chief Risk Officer since 2014, leading the enterprise risk management program and enabling the identification, prioritization, evaluation and mitigation of key risks to achieving the IRS mission. Previously, Tom was the Director of Planning and Research in the IRS's Large Business and International Division, with responsibility for the Division's workload selection and risk identification processes, and development of the annual compliance plan.

In 2016, Tom served as the Head of the Tax Administration Unit at the Organization for Economic Cooperation and Development (OECD) in Paris, France where he led the work of the Forum on Tax Administration (FTA), a unique body that brings together the leaders of tax administrations from 50 countries to enhance tax administration around the world. Tom has also provided tax administration advisory and capacity building assistance to numerous tax administrations through projects of the International Monetary Fund and OECD. Tom began federal service in 1994 as a Presidential Management Intern.

Email Address: Thomas.A.Brandt@irs.gov

Introductions and Opening Remarks

Julie Amos, WA DOR Enterprise Risk Officer

Julie has the good fortune of serving a Department that values the principles of ERM and its ability to strengthen people and improve outcomes.

Before assuming this role in April 2016, Julie served 18 years at the WA State Auditor's Office (external auditor of public accounts), with 16 of those years in supervisory and management positions. Her experience with risk-based performance audits, financial and federal audits has been invaluable in her current position.

Julie is certified in Risk Management Assurance (CRMA), is a Certified Government Audit Professional (CGAP), and has obtained the COSO Internal Control Certificate. She is frequently asked to share her ERM journey and tools with new risk officers, other state agencies, and professional groups.

Email Address: JulieA@DOR.WA.GOV

Overview of Enterprise Risk Management

Overview of Enterprise Risk Management

For the purposes of ensuring we are all using common terms in the same way this session, here are some common definitions.

What is Risk?

Risk is the **possibility** that an event will occur and affect the achievement of strategy and business objectives.

NOTE: Not all risks are bad and sometimes taking risks is worth the possible reward.

What is Risk Management?

Risk management is the process by which management identifies, assesses, manages and monitors risk.

- This includes decisions about which risks to accept, avoid, mitigate, or transfer/share.

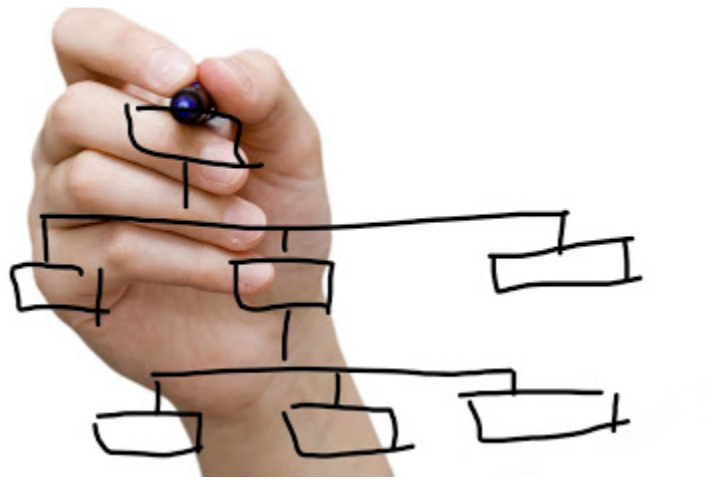
The right parties must be brought together to identify potential events, evaluate risks, and determine adequate risk responses.

Overview of Enterprise Risk Management

What is Enterprise Risk Management (ERM)

Enterprise Risk Management –The culture, capabilities, and practices integrated with strategy-setting and its performance that organizations rely on to manage risk in creating, preserving, and realizing value.

The objective of **ERM** is to support the identification and assessment of risks, and provide senior management the information necessary to make sound decisions, with risk being one of the core elements of the decision-making framework.



Overview of Enterprise Risk Management

Risk Management vs. Enterprise Risk Management

Risk Management	Enterprise Risk Management
▪ Part of **day to day business** ▪ Focused on the **business unit, program, or process level** ▪ Risks are **not assessed and reviewed together** across the organization	▪ **Holistic approach** that provides transparency at the enterprise level ▪ Considers risk management in strategy **setting across the enterprise** ▪ A portfolio view of risks to understand how individual risks **are related**

Overview of Enterprise Risk Management

Risk Occurs at Different Levels of an Organization

Lower Level Risks may Escalate to Higher Levels

Entity/Enterprise Level Risks:
Risks that affect an entire agency/organization
Example: Critical Staffing Shortages, Aging Hardware & Software

Unit Level Risks:
Risks that affect a business unit
Example: Limited call center personnel in one division

Program Level Risks:
Risks that affect a program
Example: The Employee Recognition Program is underfunded

Process Level Risks:
Risks that affect a task or process
Example: Unprocessed disbursements

Higher Level Risks may have Downstream Impacts

Note: Sometimes risks occurring at lower levels of the agency can affect higher levels of the organization depending on how serious the risk is.

ERM at the Internal Revenue Service (IRS)

ERM at the IRS

In 2013, the IRS was Under Intense Scrutiny, which Highlighted the Need to Enhance the Timely Flow of Risk Information

Background of the Crisis:

- In 2013, TIGTA uncovered that the IRS used potentially biased criteria that may have targeted certain organizations applying for tax-exempt status. The agency received backlash from oversight bodies, faced congressional scrutiny, and Significant media coverage because of the issue. The crisis revealed the need to develop the structure, processes, and mechanisms to enable the flow of risk information, up, down, and across the organization.
- In response to this crisis, IRS leadership put in place an ERM Program to provide a common framework for identifying, assessing, managing, monitoring and reporting on risks across the IRS, with the intent of improving the timeliness by which information is brought to leadership's attention as well as to increase transparency overall.

IRS

Charting a Path Forward at the IRS:
Initial Assessment and Plan of Action

Daniel Werfel, IRS

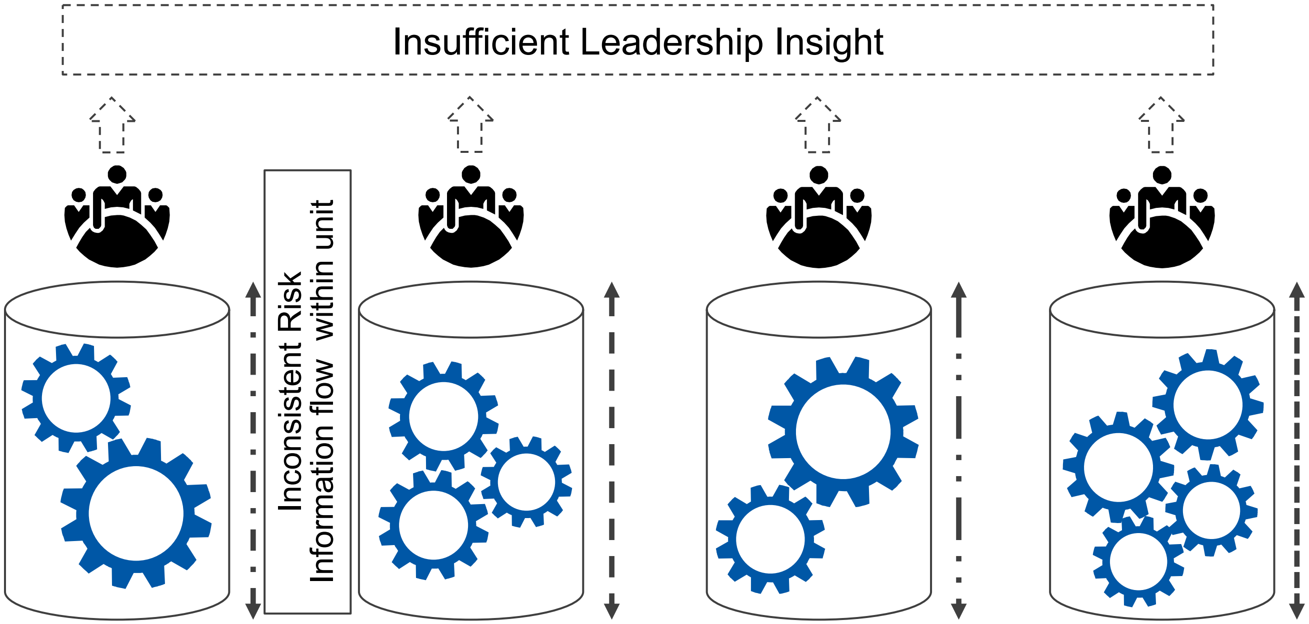
June 24, 2013

Charting a Path Forward at the IRS: Initial Assessment and Plan of Action

ERM at the IRS

Before the ERM Program was Implemented, the Flow of Risk Information was Inconsistent throughout the IRS

- No standardized approach to risk management
- Previous attempts to implement ERM did not take hold
- Hesitation to raise issues and risks
- Risks identified and managed within organizational silos without a cross-entity view or consistent approach
- Inconsistent leadership insight and limited knowledge of emerging risks among the various IRS business units
- Limited understanding of and coordinated response to risks to strategic goals and objectives
- Predominate focus on operational risk



Ad-hoc risk management within business units

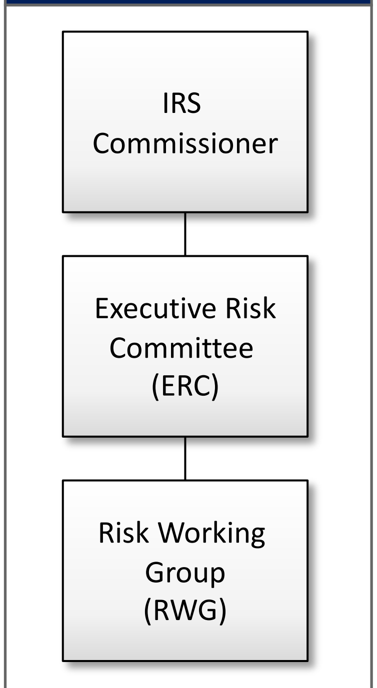
ERM at the IRS

Foundational Components and Structure of the ERM Program

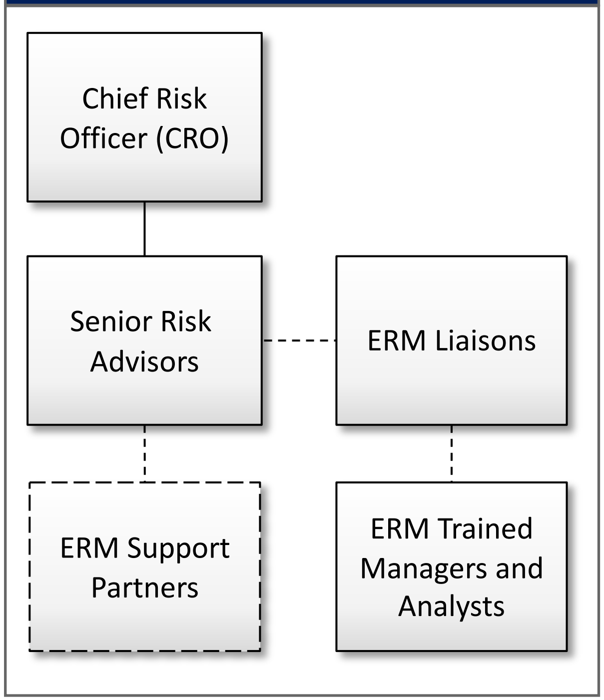
Program Objectives

Aligning risk appetite and strategy	Identifying and managing cross-enterprise risks	Enhancing enterprise risk response decisions	Reducing operational surprises	Identifying opportunities	Informing resource deployment	Supporting a risk-aware culture	Providing transparency to stakeholders

Governance Model



Operating Model



Guiding Principles

- Remains lightweight, repeatable and rapidly deployable
- Leverages existing capabilities and embeds ERM into the IRS
- Promotes effective risk communication to enable transparency and collaboration
- Recognizes that risks in and of themselves are neither good nor bad
- Supports the organization in critical focus areas
- Drives connectivity across risk priorities of the IRS
- Promotes risk based decision making

ERM at the IRS

IRS Enterprise Risk Appetite Statement

Recognizing that risk is inherent to the operations of any organization, the IRS actively identifies and manages risks to the nation’s tax administration system, with a focus on those that affect taxpayer data and the IRS mission and vision. As a large, complex, public-facing organization, the IRS acknowledges it must sometimes accept risk and uses thoughtful analysis to determine the level of risk it is willing to accept. The IRS is committed to preventing and mitigating risk exposure, particularly in areas that could affect our ability to:

- Administer the tax law fairly and with integrity,
- Protect taxpayer rights,
- Safeguard taxpayer data,
- Serve as a responsible steward of taxpayer dollars, and
- Provide an inclusive, safe and secure workplace.

Each IRS employee plays an important role in supporting the identification and management of risk.

ERM at the IRS – Example Activities

The ERM program has various activities that support the IRS in enhancing its risk management capabilities while helping provide leadership with the necessary risk information to enhance decision making.

- Enterprise Risk Assessments
- Executive Risk Committee & Risk Working Group Facilitation
- Operationalization of RM Standards, Self Assessments & Reviews
- Incorporation of Enterprise Risks into Strategic & Investment Planning Processes
- Enterprise Risk Indicators
- ERM Processes, Tools, and Templates
- Communications & Trainings
- Fraud Risk Roundtable Facilitation
- Partner to Support Units with RM Initiatives
- Representation of Risk Perspective in Existing Committees & Working Groups

ERM at the IRS

Overview of Annual Enterprise Risk Assessment Process

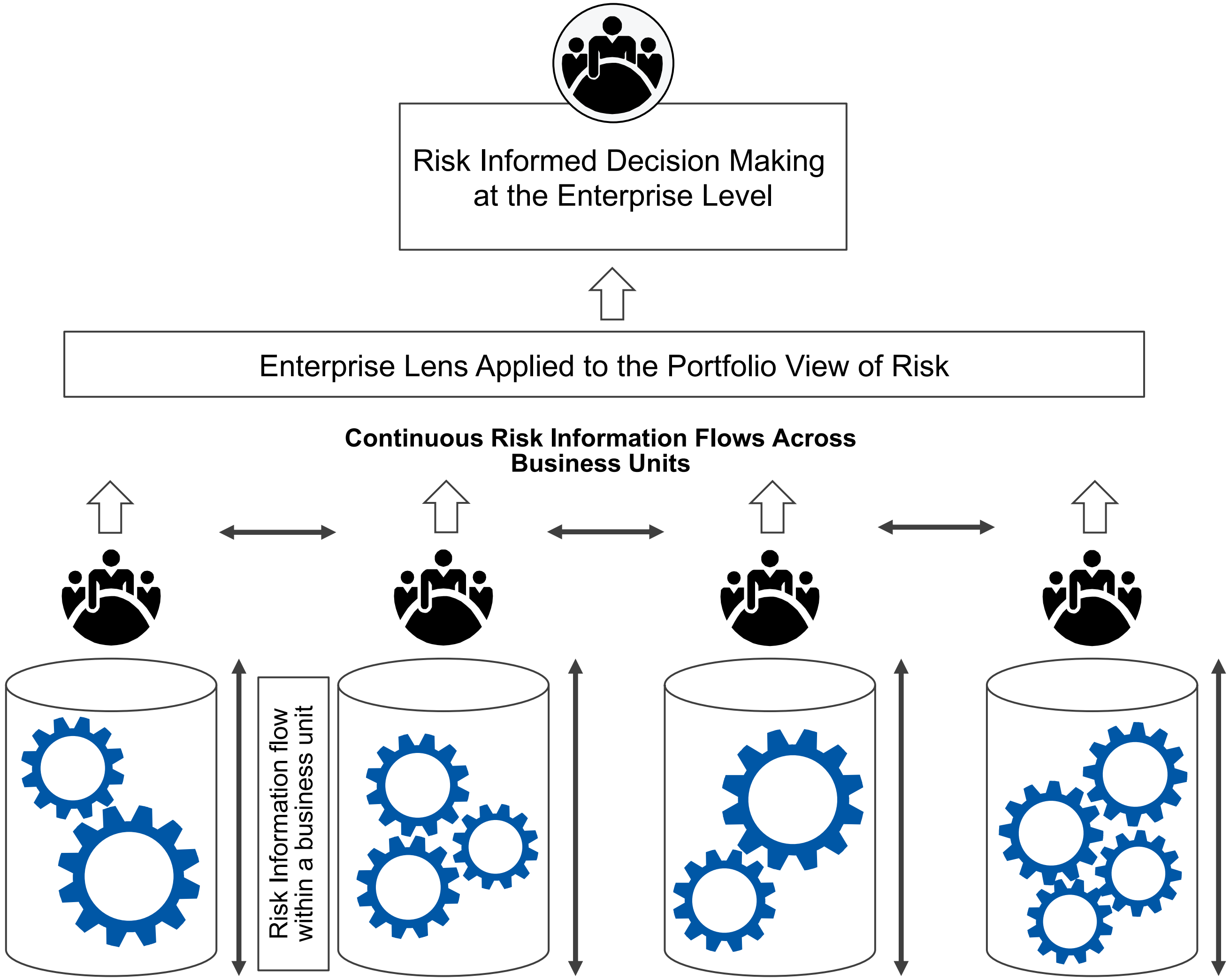
Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
ERM Liaisons submit: • Unit risk registers; • Templates indicating if each 2018/19 enterprise risk should remain on the enterprise risk list, input on the future outlook of the risks, & any risks that should be added. OCRO aggregates updates on enterprise risks from accountable parties' Business Process Reviews (BPRs).	RWG meets to: •Review aggregated risk information, •Identify any changes that should be made to the enterprise risk list, •Discuss the future outlook of the risks, •Discuss the mitigation strategies for each of the risks & identify potential exposures, & •Identify any additional information that should be gathered & provided to the ERC, as necessary.	The Accountable Parties will: •Score their respective enterprise risk(s), & •Provide any additional updates as necessary. Each ERM Liaison meets with their head of office to determine whether they believe each risk requires additional focus.	ERC meets to: •Review initial enterprise risk assessment outputs, •Agree on any changes, •Determine which risks require additional focus over the next year, & •Assign accountable parties to develop recommendations to address risk requiring additional focus.	Accountable parties identified for the risks selected by the ERC for additional focus: •Develop recommendations for additional actions, with support from OCRO, & •Develop materials to support presentation of recommendations to the ERC.	ERC meets to: •Review additional actions recommended by accountable parties, & •Determine associated next steps.

ERM at the IRS – ERM Value Realized

ERM Provides Value to the IRS by Supporting the Flow of Risk Information and Risk Informed Decision Making at Each Level

Benefits of ERM

- Increase the range of opportunities for the Service
- Increase positive outcomes and advantages while reducing negative surprises
- Identify and manage Service-wide risks
- Reduce performance variability
- Improve resource deployment
- Provide expanded view of areas of risk



ERM at the IRS – Capability Model

Foundational

- "Tone at the top" is set
- ERM Governance & Operating Model defined & implemented
- ERM Liaisons established within business units
- Operating unit risks are included in BPRs & other governance processes
- Initial high-level enterprise risk identification & assessment performed
- Enterprise risk training provided to key ERM stakeholders

Standardized

- Process to set risk appetite
- Strategic Goals developed
- Key ERM policies & procedures developed
- Enterprise Risk Assessment Approach defined & assessments occur annually
- RM guidance, standards, tools, & templates provided
- Framework provided for considering risk in key business decisions
- Guidance provided on the use of indicators to help with managing risk
- RM training / communication provided to all employees

Integrated

- Risk appetite defined at enterprise level
- Business unit objectives align to Strategic Goals
- Enterprise risk information informs IRS's & business unit Strategic Planning processes
- Scenario analysis is used to identify risks
- Stand-alone risk assessment processes connect to enterprise risk assessment through business unit risk registers
- Framework to consider risk in key business decisions widely adopted
- Enterprise risk responses are determined in alignment w/ appetite & strategy
- Enterprise risk indicators are defined and monitored
- Tone at the middle is supportive of ERM & RM
- RM is operationalized in most business units
- Service-wide understanding of the connection between risk appetite and responses
- Emerging risks actively identified and considered

Sustaining

- Enterprise Risk Assessment cycle is integrated with IRS' Strategic Planning Process
- Enterprise risks identified, assessed & reported timely
- RM is operationalized across business units
- Policies, procedures, & processes at all levels reflect risk appetite & strategy
- Effectiveness of mitigations (e.g. A-123 and other testing) considered as part of Integrated Strategic Planning & Risk Assessment Cycle
- Risk indicators are actively monitored in the context of risk appetite and performance
- Employees at all levels feel comfortable communicating openly about risks
- ERM Program performance is actively monitored & reported
- Consistent risk identification and assessment processes are integrated throughout the organization
- Performance, risks, & culture are collectively monitored & reported at the enterprise level
- Lookback analyses consistently performed when a risk manifests into an issue to determine areas for enhancement

NOTE: Capabilities are contingent upon various dependencies, such as: resources and related prioritization, objective setting processes and protocols, operationalization of RM within the operating units, scope of A-123 and other testing activities, continued dedication of future leadership, and a supportive organizational culture.

ERM at the IRS – Capability Model

This view of the IRS Capability Model identifies desired attributes of the ERM Program based on the COSO ERM Framework.

COSO ERM Framework Components	Desired Attributes Of ERM At The IRS
Governance & Culture	• Management provides a safe environment and forum for risks to be identified and discussed • Risk Appetite is established by the Senior Executive Team and cascades through the business units • Risk Management expectations are set and performance incentives reinforce the expectations
Strategy & Objective Setting	• Risk is a key input into the strategic planning and objective setting process • Strategic objectives are clearly defined at the enterprise level and cascade/align to the business unit level objectives • Strategic plans/objectives are reviewed and revised, as necessary, on a cyclical basis
Performance	• Risks to strategic objectives are identified cross-organizationally, and the Strategic Planning Process considers risks identified • Numerous mechanisms are in place to identify risks from both a top-down and bottom-up perspective and escalate, as appropriate • Internal and external factors are considered when identifying risks • Business unit risk registers reflect the current state of their business • Emerging risks are actively identified and considered

ERM at the IRS – Capability Model

Risk Maturity/Capability Model Discussion (continued)

COSO ERM Framework Components	Desired Attributes Of ERM At The IRS
Performance *(continued)*	• Enterprise risk assessments are objectives based, leveraging a robust set of risk categories, and risk is assessed cross-organizationally • Enterprise risk assessments maintain attributes of both a top-down and bottom-up risk assessment, including consideration of external events • Outputs from risk assessments at the unit level and the process level, as well as other risk assessments are used as inputs to higher risk assessments (e.g. enterprise risk assessment) • Process level risk assessments inform control design for new and changing processes • Enterprise risk responses are determined in alignment with appetite & strategy • Risk responses are appropriately documented and prioritized • Risks are assigned owners • Identification, tracking and analysis is performed cross-organizationally • Risks and control objectives are appropriately documented in policies and procedures

ERM at the IRS – Capability Model

Risk Maturity/Capability Model Discussion (continued)

COSO ERM Framework Components	Desired Attributes Of ERM At The IRS
Information, Communication & Reporting	• ERM provides management with real-time access to risk information, brings the information together and identifies themes, leveraging both lagging and leading indicators • The roles of employees at every level as they relate to ERM have been clearly articulated to the entire organization • ERM training and certification program options exist for multiple audiences • Information regarding the status and impact of risk response strategies for enterprise risks is routinely communicated across the Service • Reports on culture are given to leadership to enhance their understanding of attitudes and behavior
Review & Revision	• Information from various sources is leveraged as risk and mitigation testing information, where appropriate • Indicators are used to identify, assess, and monitor risk in the context of performance • Risks and mitigations are tracked and monitored, including testing information such as: how often the mitigations are tested, who tests them, & results of the tests • Enterprise risks are actively monitored, including through the use of scenario analysis • Progress of the ERM Program is regularly assessed against its objectives • Monitoring approach is based on risk prioritization

ERM at the IRS – IRS 2018/19 Enterprise Risk Profile

#	Risk Name	Risk Description
1	Tax Reform Implementation	The risk that failure to timely and effectively implement and communicate tax reform could inhibit taxpayers' ability to understand and comply with their tax obligations, inhibit the IRS's ability to execute filing season and deliver its compliance plan, and erode trust and confidence in the IRS.
2	Cyber and Data Security	The risk that the increased complexity, sophistication, and volume of cyber threats, including insider threats, social engineering, and unauthorized access to sensitive information, results in data loss, refund fraud, identity theft, ransomware, or denial of service.
3	Aging Hardware and Software	The risk that aged hardware and software may cause outages or failures and inhibit the IRS's ability to successfully deliver filing season, conduct daily operations, and perform its core tax administration responsibilities.
4	Critical Staffing Shortages	The risk that increased attrition and continued constraints in hiring, onboarding, and retaining employees and managers with needed skills and expertise results in critical business failures and over-reliance on contractors.
5	Adverse Impact of Reduced Service and Enforcement on Voluntary Compliance	The risk that reduced service and/or enforcement activities may erode confidence in the tax administration system and adversely impact voluntary compliance.
6	Impact of Outdated Technology Environment on Modernization	The risk that the IRS is unable to modernize and simplify its IT architecture to keep pace with changing technology and development and service delivery methods, thereby jeopardizing the IRS's ability to deliver modernized capabilities and services.

ERM at the IRS – IRS 2018/19 Enterprise Risk Profile

#	Risk Name	Risk Description
7	Secure Access to IRS Services	The risk that the IRS does not have an effective authentication and authorization protocol that reduces individual and business identity theft and refund fraud, protects taxpayer data, and still allows legitimate taxpayers to access IRS services.
8	Data Breaches at External Entities	The risk that data breaches at external entities compromise access to tax related data elements, which may result in increased refund fraud, taxpayer burden, lost revenue, and decreased public confidence.
9	Changing and Expanding Mission	The risk that legislative or executive requirements that expand, change, or reform the IRS or its mission may impact the IRS's ability to fulfill its responsibilities.
10	New and Evolving Compliance Issues	The risk that rapidly evolving business structures and payment methods, tax reform, complex tax structures, and abusive tax schemes create opportunities for non-compliance and contribute to the tax gap.
11	Contract Acquisition and Execution	The risk that the IRS is unable to timely acquire necessary products and services, initiate work under the applicable contracts (including contractor onboarding), and effectively monitor contract execution and budget, which may result in failure to execute the mission, loss of funding, and erosion of trust in the IRS.
12	Refundable Credit-Driven Refund Fraud and Non-Compliance	The risk that refundable credits create opportunities for refund fraud and lost revenue.
13	Employee Engagement and Morale	The risk that not adequately addressing key employee engagement factors, such as continued increased workload with fewer resources, increasing need to rely on acting and temporary managers, and a challenging external environment, may result in lower performance, morale, and engagement.

ERM at the IRS – IRS 2018/19 Enterprise Risk Profile

#	Risk Name	Risk Description
14	Record Retention and Document Production	The risk that an inability to effectively capture, retain, and produce hard and soft copy documents and data creates delayed, incomplete, or inaccurate responses to internal and external requests for information and adversely impacts litigation.
15	Data Access and Analytics	The risk that insufficient ability to manage, access, and analyze data the IRS captures and maintains inhibits the IRS's ability to accomplish compliance objectives, improve decision making, and provide quality service, while also increasing the potential for data exposure and creating unnecessary burden on taxpayers.
16	Digital Service	The risk that the inability to effectively and securely deploy and maintain resilient digital and virtual service may result in unintended consequences such as: a failure to achieve strategic objectives, higher call volumes, new avenues for fraud, future unwillingness to use digital services, decreased voluntary compliance, and erosion of trust in the IRS.
17	Strategic Alignment and Resource Deployment	The risk that the appropriation structure, budget delays, and insufficient alignment of unit goals and objectives with IRS's strategic goals and objectives inhibit the IRS's ability to strategically deploy resources to achieve its mission.
18	Change Management	The risk that failure to provide IRS managers and employees with the capabilities and tools needed to effectively plan, communicate, and embrace change may result in an inability to implement organizational objectives and could have a negative impact in areas such as employee morale, culture, and program effectiveness.
19	Vendor and Third Party Actions Inconsistent with IRS Standards	The risk that vendors and other third parties acting on behalf of or providing services for the IRS may act in a manner inconsistent with IRS standards, which may reflect negatively on the IRS and erode public trust and confidence in the IRS and tax administration.

ERM at the IRS – IRS 2018/19 Enterprise Risk Profile

#	Risk Name	Risk Description
20	Revenue Accounting	The risk that an inability to accurately report revenues and properly calculate and maintain taxpayer accounts may erode confidence in the IRS and tax administration.
21	Policies, Procedures, and Internal Controls	The risk that duplicative, outdated, cumbersome, non-existent, or insufficient policies, procedures, or internal and management controls and lack of adherence to controls may result in incorrect or inconsistent execution and delivery of program goals and objectives.
22	Physical Security and Safety	The risk that the IRS is unable to ensure the safety of its people and the security of its facilities, assets, and information from internal and external threats.
23	External Engagement	The risk that failure to communicate with external stakeholders in a proactive, effective, accurate, and timely manner may inhibit the IRS's ability to achieve its strategic goals and impact trust and confidence in the IRS.

Questions?

ERM at Washington State Department of Revenue (WA DOR)

ERM at WA DOR

Washington state's first wake up call…

- FY 2001 Actuary estimate was $28 million in tort payouts
- FY 2001 Actual payout **$85 million**

Then Governor Locke and Attorney General Gregiore co-sponsored a Task Force to assess state risk management issues

Key findings:

- Risks should be managed at the enterprise level
- High level review process needed for all significant losses
- Policy level visibility was needed within the budget process for loss funding requirements and loss prevention efforts

"*The ability to manage risk is an essential element of good governance" -- WA Governor Chris Gregiore*

ERM at WA DOR

Washington state's second wake up call…

Seattle Times, December 2015

…the Washington Department of Corrections has been making mistakes in calculating (prison) sentences since 2002…

For three years, state Department of Corrections staff knew a software-coding error was miscalculating prison sentences...Gov. Jay Inslee gave the damning tally: up to 3,200 prisoners set free too soon since 2002.

…Department of Corrections analysis (of CY15) said (it) affected about 3 percent of all releases…offenders were released from prison an average 55 days before their correct release dates

Gov. Inslee's Executive Order 16-06 *…managing risk cannot be done by any one individual, department, or agency but must be ingrained in all state agencies at all levels…*

ERM at WA DOR

ERM Program Objectives

Dialogue	Strengthen Risk Owner dialogue with Executives and Leadership Break down silos Knowledge transfer
Alignment	Align strategy, resources and risk culture with the desired risk appetite
Proactive Management	Enable proactive risk identification and responses
Strengthen Capabilities	Update risk management capabilities to address an ever changing business environment with impacts crossing divisions

ERM at WA DOR

Expected ERM Outcomes	
Dialogue	Executives and Leadership have regular, and value-added, updates on the risks of greatest importance Improved risk management continuity when turnover occurs
Alignment	Allow for calculated risks and promote deliberate innovation Protect the Department’s reputation
Proactive Management	Improved likelihood of achieving strategic and performance outcomes Reduced impact and/or duration of threats and weaknesses
Strengthen Capabilities	Continued growth of the Department’s risk culture, risk awareness and risk monitoring capabilities

ERM at WA DOR

Enterprise Approach to "Who Does What"

IIA's - Three Lines of Defense

1st	Business Lines and Functions	"Own" the risks associated with their activities and execute risk management processes
2nd	Risk Management	Designs & coordinates the implementation of the ERM program
3rd	Internal Audit	Validates the effectiveness of the ERM program

ERM at WA DOR

Our Risk Owners know their stuff!

ERM at WA DOR

ERO Responsibilities

DOR Administrative Policy 1.3.2 – Managing Enterprise Risk

Enterprise Risk Officer (ERO)	• Maintain and mature Revenue's ERM framework and policy. • Facilitate enterprise risk identification and risk assessments as needed. • Verify that mission-critical risk treatment activities are monitored and appear effective. • Coordinate risk management training.

ERM at WA DOR

Risk Management Maturity *(1 of 2)*			
Level	**Initial**	**Pilot**	**Repeatable**
Description	Development stage	Initial enterprise-wide risk assessments	Process established and repeatable
Activities	Define common terminology Define roles & responsibilities Create a framework Establish steering committee	Create templates & tools to support ERM framework: • Risk assessment • Risk matrix (heat map) • Risk register • Risk categories Develop training ERO facilitates enterprise, project-based & internal control risk assessments	Increased use of assessment tools Continued education and outreach Efforts to integrate priority risks with budget & strategic planning

ERM at WA DOR

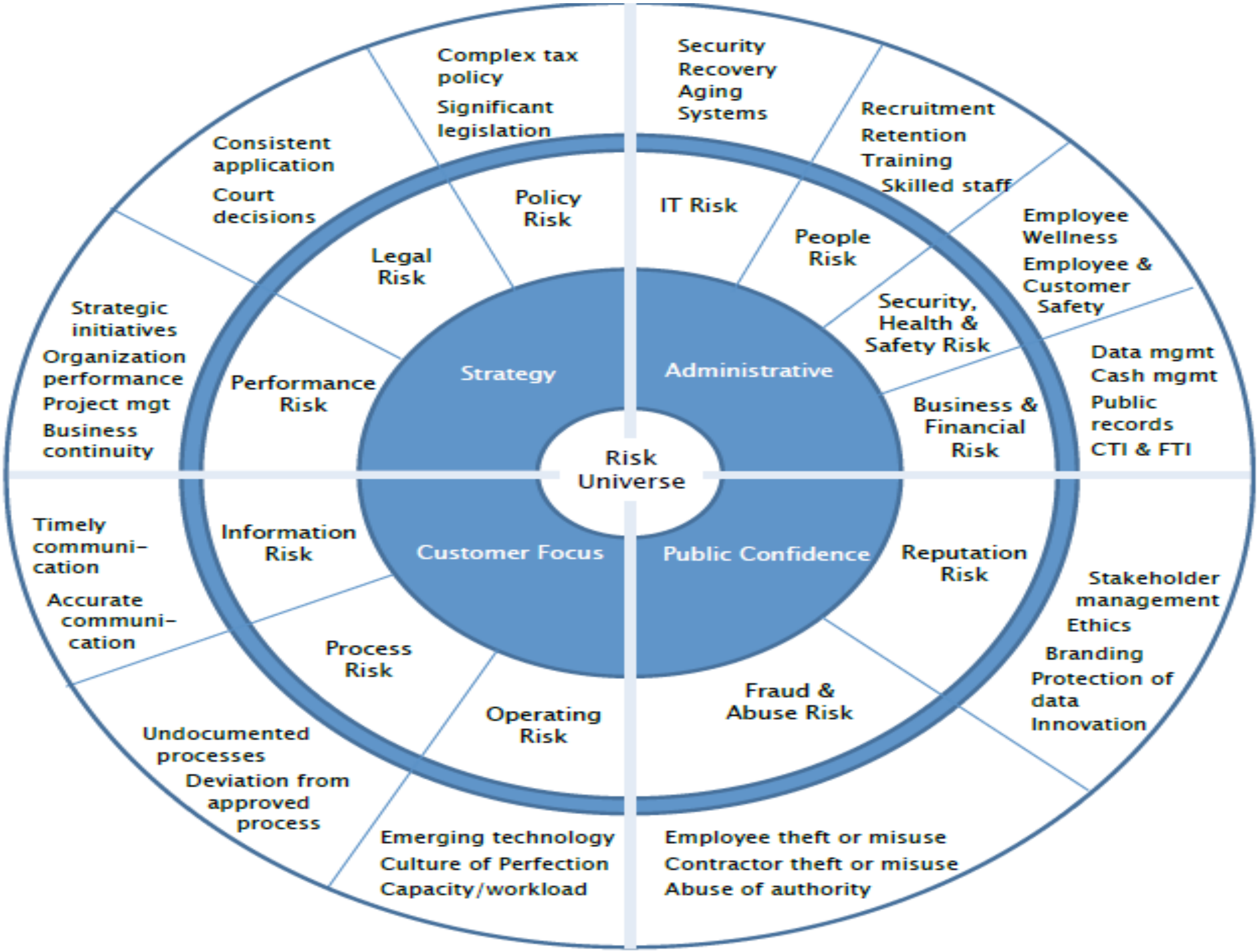
Risk Management Maturity *(2 of 2)*			
Level	**Defined**	**Managed**	**Optimizing**
Description	General awareness of risks' connection to outcomes	Regular risk assessments and risk monitoring	Continuous feedback Performance improvement
Activities	Establish ERM policy & risk appetite statement Develop Priority Risk Register Develop risk appetite training for Executives Risks integrated with budget, SBP, and priority initiatives	Risk Owners monitor risks according to treatment plan Risk Owner progress reports to Leadership Team Priority Risk Owners develop & monitor key risk indicators (KRI's); quarterly reports to Executive Team	Optimized KRI & KPI use for real-time risk analysis of changing risk exposure Monitor mitigations for effectiveness Monitor indicators for consistent, relevant, and reliable development and application

ERM at WA DOR

Risk Owners Report Progress

2013 Risk ID	Risk Title	Risk Owner	2013 Heat Map Score	2015 Heat Map Score	2015 Treatment		2017 Inherent / Residual	Likelihood	Impact	2017 Preliminary Heat Map Score
3b	Retention	Steve McLain	16	20	Reduce	RO Pick	Inherent Risk	[illegible]	[illegible]	High
							ACTUAL Residual Risk	3. Possible	3. Major	Medium
							TARGET Residual Risk	3. Possible	2. Minor	Medium
						Voter Pick	Inherent Risk			
							ACTUAL Residual Risk			
							TARGET Residual Risk			

ERM at WA DOR


Risk Universe
Strategy
Administrative
Customer Focus
Public Confidence
Policy Risk
Legal Risk
Performance Risk
IT Risk
People Risk
Security, Health & Safety Risk
Business & Financial Risk
Information Risk
Process Risk
Operating Risk
Reputation Risk
Fraud & Abuse Risk
Complex tax policy
Significant legislation
Consistent application
Court decisions
Strategic initiatives
Organization performance
Project mgt
Business continuity
Security
Recovery
Aging
Systems
Recruitment
Retention
Training
Skilled staff
Employee Wellness
Employee & Customer Safety
Data mgmt
Cash mgmt
Public records
CTI & FTI
Timely communi-cation
Accurate communi-cation
Undocumented processes
Deviation from approved process
Emerging technology
Culture of Perfection
Capacity/workload
Employee theft or misuse
Contractor theft or misuse
Abuse of authority
Stakeholder management
Ethics
Branding
Protection of data
Innovation

ERM at WA DOR

WA DOR Enterprise Risk Register – Top 6		
Risk Name	**Risk Treatment**	**Risk Treatment Plan – FY19**
System Security	Reduce	• Proactively monitor systems • Continue system risk assessments • Maintain training and staffing of security office • Annual reviews of user access • Eliminate unneeded system access • Continue staff security training
Complex Tax Policy	Accept & Monitor	• Continue centralized tax policy development • Continue internal & external tax policy guidance • Continue to monitor and escalate significant complex tax policy issues to the Department's leadership
Legacy Replacement	Reduce	• OCIO oversight & comprehensive decision process • Quality assurance & change management consultants • Frequent project reporting on progress and risk identification; code freeze dates by functional area • Etc.

ERM at WA DOR

WA DOR Enterprise Risk Register – Top 6		
Risk Name	**Risk Treatment**	**Risk Treatment Plan – FY19**
Aging I.T. Systems	Reduce	• Upgrade or replace priority aging systems/capabilities • Maintain tactical roadmap • Ensure telephony systems are standardized, consolidated, and stabilized
Managing Public Records	Reduce	• Continue Public Records training for all new employees and refresher training every two years. • Implement software for public records requests • Develop tool to improve documentation of Public Records searches
Protecting Confidential Information	Reduce	• Require second technical review before release • Update Privacy Training for those with access to CTI • Minimize the collection and retention of CTI • Improve confidentiality / breach procedures • Review data share agreements for alignment with requirements

ERM at WA DOR

2016 Common Priority Risks across WA State Agencies	
Risk Name	**Examples Cited**
Agency Funding	*No explanation needed….*
Employee Risks	Recruitment Retention Morale Succession planning Workloads
I.T. Risks	IT security / confidential data Legacy systems

ERM at WA DOR

Take Aways

- Start simple
- Creating an ERM program is a journey, not a destination
- Set the tone from the top
- Customize existing resources and tools

- Sharing risks doesn't have to be risky!
  - Improves stakeholder confidence – you know your top risks
  - Improves peer-to-peer communication and learning – you're not alone

Risks to Tax Administration from a Global Perspective

Risks to Tax Administration from a Global Perspective

Background

- The Organisation for Economic Co-operation and Development (OECD) Forum on Tax Administration (FTA) was created in 2002 and is a unique forum on tax administration for Commissioners from 53 OECD and non-OECD countries, including members of the G20.
- A discussion about risks at the September 2017 meeting led to the creation of the OECD FTA Risk Management Community of Interest (COI), which is currently led by the IRS and chaired by the IRS Chief Risk Officer, Tom Brandt.
- The second annual Risk Workshop was held in April 2019 and covered topics such as reputational risk, internal control and ERM, capability models for ERM, risk identification and mitigation methods and approaches, key risk indicators, emerging risks and lessons learned from risk events.
- The following slides provide the most recent top risk themes facing tax administrations around the world.

Risks to Tax Administration from a Global Perspective

Top Risks Facing OECD Tax Administrations

Including associated areas of risk for each theme

Theme	Areas of risk	
Tax Non-Compliance and Fraud (1)	• New and evolving compliance issues • Non-compliance in the financial markets • Non-payment/untimely payment of taxes • Legal loopholes • Refund fraud	• False or fictitious ID's in the population register • International tax and VAT fraud • Tax evasion related to internal taxes and foreign trade • Evasion and/or avoidance
Human Capital (2)	• Critical staffing shortages • Capacity, capabilities, and engagement of staff • Loss of key competencies in the tax authority • Rapidly evolving employment market	• Employment framework and conditions, and competitor offers, which impact the ability to attract and retain employees • Maintaining trained employees and the burnout of experienced employees
Cyber and Data Security (3)	• Cyber security threats • Data and information assets held are unavailable due to cyber threats • Data protection	• Protection of taxpayer information • Information security

Risks to Tax Administration from a Global Perspective

Top Risks Facing OECD Tax Administrations

Including associated areas of risk for each theme

Reputation and Trust (4)

- Integrity/Ethical infrastructure
- Unexpected negative customer reaction to changes
- Loss of public trust and credibility
- Unfair treatment of taxpayers
- Impact on levels of trust and confidence in the tax system
- Unfair treatment of taxpayers
- External perception/loss of trust
- Equal treatment
- Unexpected negative reaction to changes

Enforcement and the Tax Law (5)

- Lack of enforcement
- Adverse impact of reduced service and enforcement on voluntary compliance
- Tax monitoring
- Investigation and prosecution
- Inability to collect tax debts in full
- Taxpayer audit
- Tax collection and recovery
- Tax audit rating

Information Technology (6)

- Delayed IT support
- Technology development
- Tax system modernization
- Outdated hardware/software
- Insufficiently renewed hardware/software
- Complicated management of existing information systems due to different technological solutions
- Scale and scope of IT projects

Risks to Tax Administration from a Global Perspective

Top Risks Facing OECD Tax Administrations

Including associated areas of risk for each theme

E-Commerce/ Digitalization 7	• Internet commerce • Digitalization of the economy • New developments in the digital environment • Control of digital economy/globalization	• Cryptocurrencies and other exotic instruments • New systems with potential to hide capital • Emerging technology, e.g. blockchain
Service to Taxpayers 8	• Adverse impact of reduced service • Products, services, and systems enhancing the taxpayer experience	• Service delivery • Service channels • Insufficient tax education and culture of compliance and citizenship
Shadow Economy 9	• Ensuring revenue is not effected by risks such as the shadow economy, off-grid tax payers, etc. • Illicit trade and smuggling • Increase in volume of organized tax crime	• Black economy • Parallel communities • Strengthening the control activity and tackle shadow economy

Risks to Tax Administration from a Global Perspective

Top Risks Facing OECD Tax Administrations

Including associated areas of risk for each theme

Theme	Associated areas of risk	
Continuity of Operations 10	• Inability to ensure continuity of operations • Business interruption • Reliability of call center hardware and software	• Catastrophic loss of buildings and/or services • Continuity of the organization due to internal, political developments in society
Globalization 11	• International administrative assistance • Decreased proceeds linked to international transactions • International context	• Globalization of the economy • Cross-border transactions • International tax competitiveness

Breakout Group Activity

Breakout Group Activity Overview

Instructions

- Break out into 4 groups, there is an assigned facilitator for each group.
- Use the provided worksheet, which includes a list of common areas of risk faced by tax administrations, to respond to the following questions individually:
  - What do you feel are the top 3-5 areas of risk facing your organization?
  - Are you interested in information about actions other tax administrations are using to respond to these risks?
- As a group, share your top risk areas and discuss the follow questions.
  - In your view, what is the impact of these risks manifesting?
  - What are some key actions you are currently taking or planning to take to respond to these risks?

Discussion of Results from Group Activity

Closing Remarks