Compliance/Internal Control Risk Assessment Framework and Methodology

Revised: April 16, 2021

What are Compliance and Internal Control Risks?

Compliance risks are the threats posed to the University when laws, regulations, or contractual agreements are violated or when effective internal controls are not in place to protect against ethical violations or fraud.

If risks are not identified, mitigated, and monitored, they can have a significant legal, financial, operational, reputational, and strategic impact on the University.

How is a Compliance Risk Assessment Different from an Enterprise or Internal Audit Risk Assessment?

While an enterprise risk assessment (ERM) and an internal audit (IA) risk assessment typically include compliance-related risks, neither is designed to solely assess regulatory or internal control areas to the level it should be reviewed and provide adequate assurance to leadership.

To effectively utilize University resources and to have a streamlined approach to mitigating risk, Western coordinates the compliance and internal control (C/IC) risk assessment process with other University areas of compliance, enterprise risk management, internal controls, ethics, and internal audit to conduct a multi-purpose review.

The interrelationship between Enterprise Risk Management (ERM), Internal Audit, Compliance, and Internal Control risk assessments.

	ERM	Internal Audit	Compliance	Internal Controls
Objective	Identify, prioritize, and assign accountability for managing strategic, operational, financial, and reputational risks	Determine and prioritize risks to aid in developing the internal audit plan, helping to provide the board and the executive leadership with assurances related to risk management efforts and other compliance activities.	Identify, prioritize, and assign accountability for managing existing or potential threats related to legal or policy noncompliance—or ethical misconduct—that could lead to fines or penalties, reputational damage, or the inability to operate competitively.	Identify, analyze, and respond to risks, including fraud, that could significantly impact the university's system of internal control and to provide the BOT and executive leadership with reasonable assurance regarding the achievement of the university's objectives relating to operations, reporting, and compliance.
Scope	Any risk significantly impacting the organization's ability to achieve its strategic objectives	Financial statement and internal control risks, as well as some operational and compliance risks that are likely to materially impact the performance of the enterprise or financial statements	Laws and regulations with which the organization is required to comply in all jurisdictions where it conducts business, as well as critical organizational policies—whether or not those policies are based on legal requirements	
Owner	Director of Risk, Compliance, and Policy Services	Internal Auditor/Ethics Officer	Director of Risk, Compliance, and Policy Services	Internal Controls Officer

Risk Assessment Framework

Guiding Principles

To better position itself strategically, the University has moved from managing compliance in a siloed, check-the-box and reactive approach to one that is proactive and collaborative, risk-based and evaluated on effectiveness.

The University C/IC risk assessment framework is based upon the:

- Department of Justice's Elements of an Effective Compliance Program 2019 – Risk Assessments
- Washington State Internal Control Policies (Chp 20) – Risk Assessments
- Compliance Risk Management: Applying the COSO ERM Framework (November 2020)
- Western Washington University's Enterprise Risk Management Framework

University Compliance Risk Landscape

The University has identified its compliance risk landscape in the form of a comprehensive University Compliance Matrix which organizes its regulatory risk areas into specific compliance categories with a delegated Compliance Owner reporting up to a Division Executive Officer.

The risk landscape also includes the maturity of the University's Compliance and Internal Controls Program ("Program") which is responsible for establishing a central resource to support individual compliance owners in implementing federal and state requirements to ensure effectiveness in mitigating compliance risk.

Risk Assessment Objectives

- Identify new or obsolete compliance areas to update the University's compliance matrix,
- Identify real and potential weaknesses (or key risk indicators - KRI's) and opportunities within the individual C/IC areas and within the Program,
- Establish action plans for high risk areas for leadership and the BOT to monitor closely,
- Provide a baseline against which future performance can be measured.

Methodology

In fiscal year (FY) 2021, the University re-designed its C/IC risk assessment methodology with a more comprehensive approach that includes a high-level risk assessment conducted on an annual basis and in-depth risk assessment conducted no longer than every 3 years.

The high-level review may include a(n):

- Employee and management survey the effectiveness of Western's compliance, ethics, and internal control activities of selected compliance and internal control areas
- Progress review of the Program
- Progress review of previous risk mitigation plans
- Review of external factors (e.g. new regulations, trending compliance issues)
- Compliance owner survey of emergent issues
- Maturity status of the Program

The in-depth review may include, in addition to activities listed above a(n):

- In-depth review of internal activities and metrics (see internal data sources below)
- Compliance owner self-assessment of the required program elements
- Risk assessment of the individual compliance and internal control areas
- Review of internal control effectiveness metrics

Internal and External Data Sources

Internal data sources to be considered:

- Employee surveys and interviews
- Compliance owner and financial manager surveys and interviews
- Internal audits and special investigation reports
- Audits and investigations by external entities
- Employee disciplinary records (Human Resources; Provost Office)
- Office of civil rights complaints/investigations
- Hotline calls
- Third-party contract performance reports
- Employee exit interviews
- Compliance program maturity assessments
- Technology/processes for compliance risk management
- Liability claims (torts)

External data sources to be considered:

- National risk rating reports
- State Internal Audit accountability audits and special audits conducted on WWU and other entities
- State Ethics Board violations report
- Compliance, Internal Controls and Risk Professional Organizations Communications and Reports
- Media sources - current events
- Federal and State Audit/Investigation Reports conducted on WWU and other entities

Reporting

An annual Compliance and Internal Controls Risk Assessment Report will be provided to the University Compliance Committee, the Provost and Vice Presidents, and the Board of Trustees. The report will include at a minimum:

- The University's Compliance and Internal Control Risk Profile (summary of prioritized risks),
- The status of the University Compliance and Internal Control Program maturity level, and
- Action plans that outlines the mitigation strategies to reduce or eliminate the risks with a specified completion target date, and
- A list of other identified risks of lower priority.

The University's annual Compliance and Internal Control Risk Profile will be submitted to the state Office of Financial Management.