Internal Control at OSU
COSO & Enterprise Risk Management

Oregon State University
Board of Trustees Executive & Audit Committee
Educational Session
The COSO framework defines **internal control** as a process, effected by an entity’s board of directors, management and other personnel, designed to provide **reasonable assurance** regarding the achievement of **objectives** in the following categories:

- Effectiveness and efficiency of **operations**
- Reliability of **financial reporting**
- **Compliance** with applicable laws and regulations
Adopted Internal Control Model

COSO provides

• OSU managers,
• external stakeholders,
• board and executive leaders, and
• internal audit

a model to evaluate operations.
Responsibility for Internal Controls

Everyone is responsible for establishing and maintaining effective internal controls...

- Faculty & staff
- Departmental management
- Central business offices
- Executive management
- Board of Trustees
- State of Oregon
Components of Internal Control

According to the COSO framework, internal control consists of five interrelated components:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring
Component 1: Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.
Component 2: Risk Assessment

A precondition to risk assessment is the establishment of objectives. Risk assessment is the identification and analysis of relevant risks to the achievement of assigned objectives.

Risk assessment is a prerequisite for determining how risks should be managed.
Component 2: Risk Types

Enterprise Risks

- Operational
- Financial
- Compliance
- Strategic
- Reputational
Component 2: Enterprise Risks

Operational: Events that impact our ability to conduct business processes, serve students, and conduct research.

Financial: Events that lead to a loss of resources needed to run operations, serve students, or conduct research.
Component 2: Enterprise Risks

**Compliance:** Events that violate laws, rules and regulations, that restrict our ability to conduct business processes, serve students, or conduct research.

**Strategic:** Directing resources towards events that do not align with the university's strategic goals and objectives.
Component 2: Enterprise Risks

**Reputational**: Events that receive negative press (national, state, local) that lead to a loss of funding, enrollment, donations, and grants.
Component 3: Control Activities

Control activities are the policies and procedures that help ensure management directives are carried out and risks are mitigated to an acceptable level.

- Policies and procedures
- Approvals and documentation
- Segregation of duties and reconciliations
- Physical and logical access controls
Component 4: Information & Communication

Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Examples include:

- Information systems, producing information that make it possible to run the university.
- Trainings, meetings, websites, newsletters, both internal and external to Oregon State
Component 5: Monitoring

Monitoring is a process that assesses the quality of the system's performance over time. Corrective actions taken ensure continuous improvement.

- Central monitoring of decentralized control activities
- Independent assurances - audits and accreditation
Internal Control Model: Next Steps

Oregon State will continue to use and improve upon the principles of COSO to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations