Powerful Insights.
Proven Delivery.®

University-wide Compliance Assessment – Phase II Results

WRIGHT STATE UNIVERSITY

December 2015

protiviti®
Risk & Business Consulting.
Internal Audit.

This report reflects the results of the Phase II effort (the recommendations phase).
Refer to separate report dated August 2015 for Phase I results (assessment phase).

Table of Contents

protiviti®

Summary of Compliance Assessment

Overall

Protiviti was engaged to perform an assessment of Wright State University's (WSU) compliance programs to analyze and document the current state of University-wide compliance. The assessment was not an audit and was not intended to evaluate the effectiveness or controls of any single law, regulation or compliance area. Rather it was an assessment of the compliance process taken as a whole. The project was broken into two phases – the Assessment Phase and the Recommendations Phase.

Phase I – Assessment Phase

Phase I results were documented in a separate report dated August 2015, which included current-state maturity assessment and observations based on the work performed.

Phase II – Recommendations Phase

Phase II included leveraging the results of the assessment phase and developing recommendations to address observations noted in Phase I. A working session was held with a cross-section of University personnel to review and further develop and document the following:

- Guiding principals surrounding University-wide Compliance development

- Desired future-state compliance maturity (after implementing recommendations)

- Recommendations (by infrastructure element), including options for University-wide organization structures for consideration

- Suggested implementation approach to address recommendations

See following pages for details on the above items.

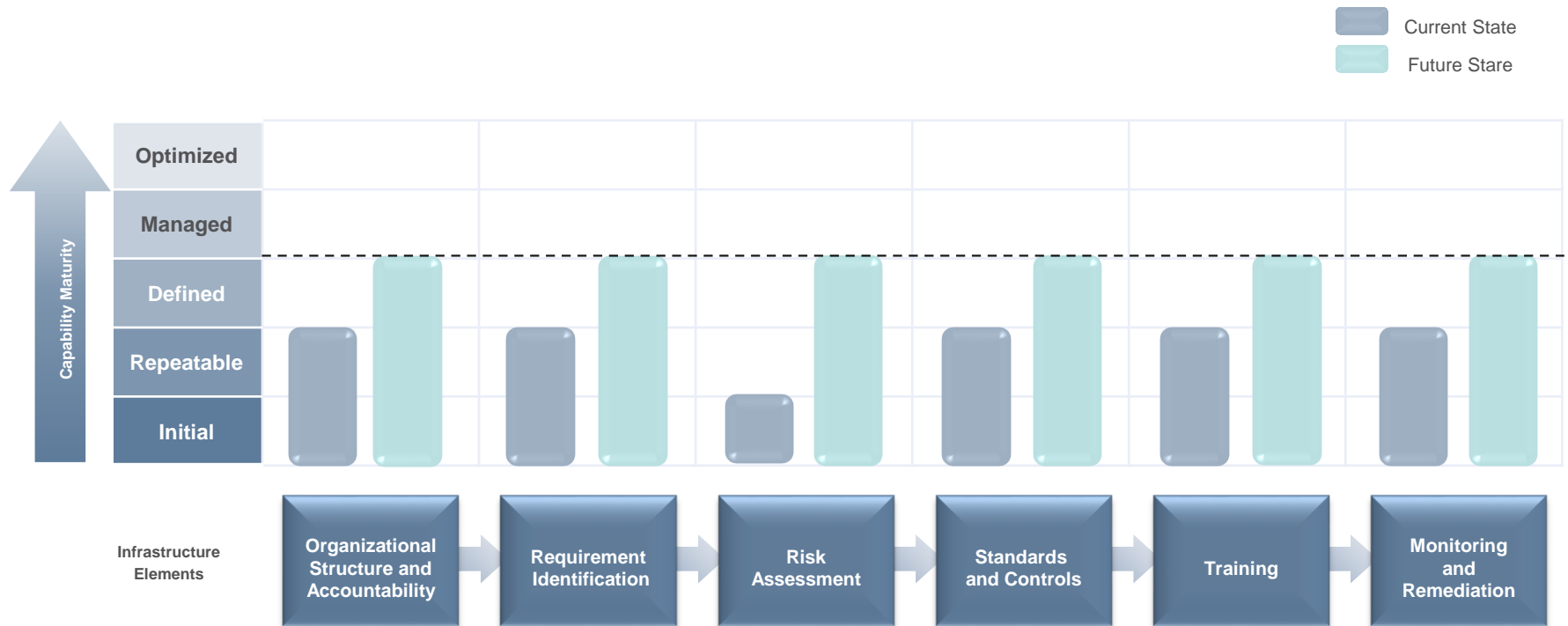protiviti®

Future State Design Development

Guiding Principles

WSU seeks a compliance function that:

- Recognizes not only the unique culture of higher education institutions, but specifically WSU's culture and embraces concepts of shared governance.

- Provides improved independence and authority for the University's compliance function, ensuring the root causes of compliance issues are effectively and timely addressed.

- Balances the University's growth as a fast moving, innovative leader with its need to adhere to the ever-changing compliance requirements.

- Has a touch point to senior leadership and the Board of Trustees.

- Can build relationships within the organization to promote, collaborate and monitor compliance.

- Can further integrate compliance into existing business processes and respond timely to department needs.

- Code of Conduct shall be consistent with and support the mission and values of the University.

protiviti®

Compliance Assessment – Desired Future Maturity State

Organizational Structure and Accountability

Current State Attributes	Key Observations	Recommendations
• Compliance is decentralized. • No University-wide oversight or coordinating function exists. • People generally encouraged to do the "Wright" thing.	• Responsibility for compliance at the Board of Trustees level is in the process of being formalized. Currently no Committee-level reporting of compliance or regular University-Wide or department level reporting exists. • A formal compliance reporting structure does not exist. Informal reporting relationships have developed in its place and reporting of issues is based largely on trust and doing the "Wright" thing. • Compliance ownership and responsibility is generally not at a strategic level and compliance issues do not appear to have a standing agenda with Senior Leadership. Involvement of General Counsel in compliance related decision making appears inconsistent. • Compliance does not appear to be a clearly stated component of process owners responsibilities and may not be documented in job descriptions.	• Formalize Board of Trustees Committee-level Compliance responsibility along with Compliance as a reporting topic. (In Progress) • Establish a University-wide Compliance Leader (level TBD) within a University Compliance Office. • Establish a University Compliance Council to support the establishment of a mature compliance function and integration into the University.

protiviti®

Organizational Structure and Accountability – Recommendation Details

Board Governance

- A formal Compliance Report should be delivered detailing the compliance activities during the period no less than quarterly to the Audit (and Compliance) Committee of the Board of Trustees.
- Board committee should have documented responsibilities surrounding Compliance (charter).
- Consider a Board member training plan related to the compliance program.

University-Wide Compliance Leader Responsibilities

- Be independent of finance / operations; reporting lines to Audit (and Compliance) Committee.
- Define an organizational compliance strategy.
- Execute the University's vision for a university-wide compliance function.
- Integrate compliance into existing business processes.
- Develop staff, as appropriate, in University Compliance office to support Compliance leader in areas of: policies & procedures, training, monitoring and investigations.
- Operate currently existing Anonymous Reporting Line(s) including investigations, as necessary.
- Define new corporate compliance processes and policies, including monitoring and remediation of compliance objectives.
- Define owners of compliance within each compliance area. Incorporate compliance expectations into job descriptions and the employee annual review process.
- Develop and initiate compliance training to increase awareness and education.

protiviti®

Organizational Structure and Accountability – Recommendation Details (continued)

Compliance Council

- Form a University Compliance Council, lead by the Compliance Leader.

- Includes the following:

  - Unit Compliance managers / directors

  - Risk Management

  - Internal Audit

  - General Counsel / Legal affairs

  - Faculty and staff representative

- Meet on a regular basis / possibly monthly to get started.

- Document the Council's mission in a charter:

  - Ensure University-wide standards for compliance have been effectively and consistently implemented.

  - Ensure compliance requirements impacting more than one function have been identified and comprehensively addressed.

  - Provide a mechanism to allow compliance leading practices to be identified and disseminated across the University (including tools).

  - Identify compliance priorities and share resources.

protiviti®

University Compliance Office

Board of Trustees

Audit (and Compliance) Committee

President

University Compliance Office
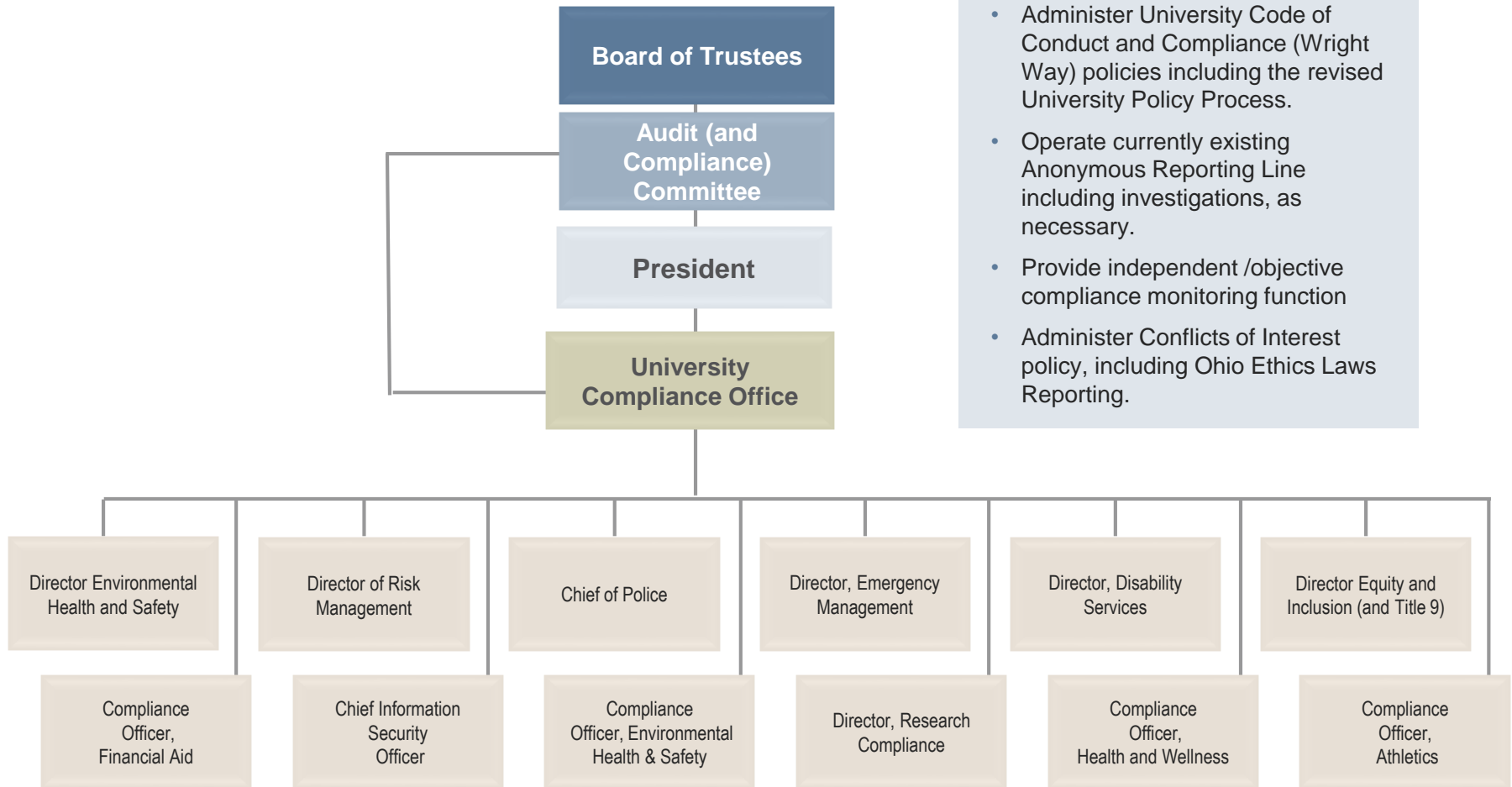
Primary Responsibilities:

- Administer University Code of Conduct and Compliance (Wright Way) policies including the revised University Policy Process.

- Operate currently existing Anonymous Reporting Line including investigations, as necessary.

- Provide independent /objective compliance monitoring function

- Administer Conflicts of Interest policy, including Ohio Ethics Laws Reporting.

| Director Environmental Health and Safety | Director of Risk Management | Chief of Police | Director, Emergency Management | Director, Disability Services | Director Equity and Inclusion (and Title 9) |

| Compliance Officer, Financial Aid | Chief Information Security Officer | Compliance Officer, Environmental Health & Safety | Director, Research Compliance | Compliance Officer, Health and Wellness | Compliance Officer, Athletics |

protiviti®

Future Compliance Organization Structure:
Leadership – Option 1 – Chief Compliance Officer Model

```
┌──────────────────────┐
│  Audit (and          │────────────────────────────────────────────┐
│  Compliance)         │                                            │
│  Committee           │                                            │
└──────────────────────┘                                            │
        │          ┌──────────────────┐                             │
        │          │   President      │                             │
        │          └──────────────────┘                             │
        │                   │                                       │
┌──────────────────────┐    │    ┌──────────────┐  ┌──────────────┐
│  Compliance          │    │    │   Chief      │  │   Internal   │
│  Leader              │  ┌─────┐ │  Operating   │  │   Audit      │
│  (Chief Compliance   │  │General│ │  Officer    │  │              │
│  Officer)            │  │Counsel│ └──────────────┘  └──────────────┘
└──────────────────────┘  └─────┘
```
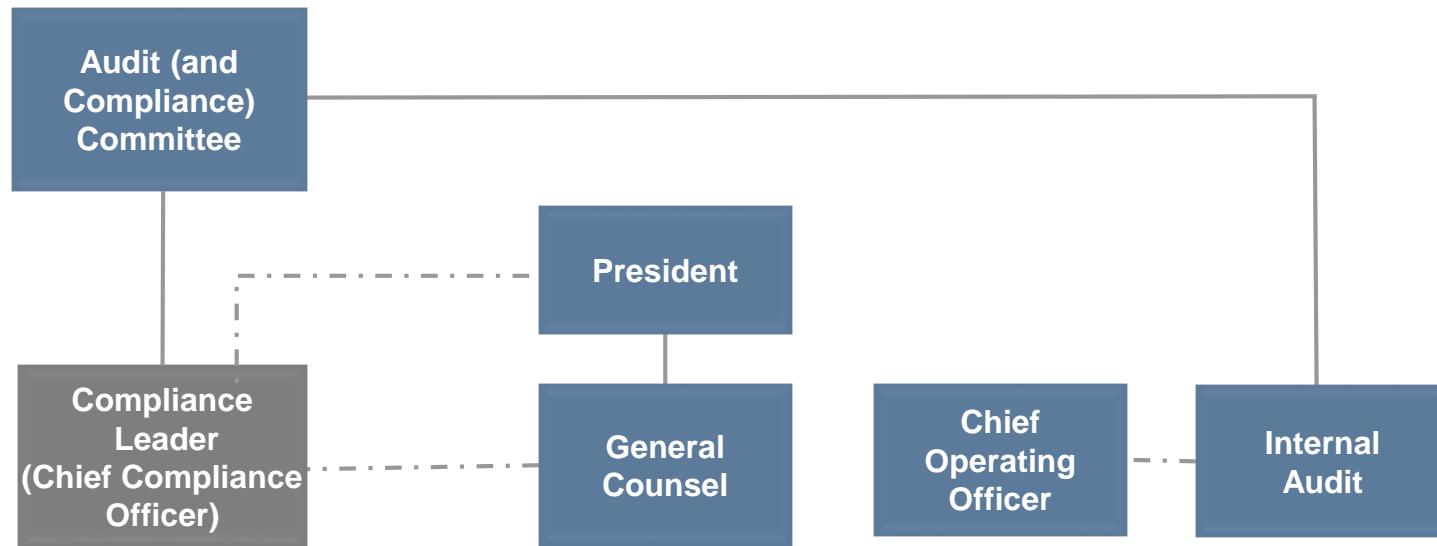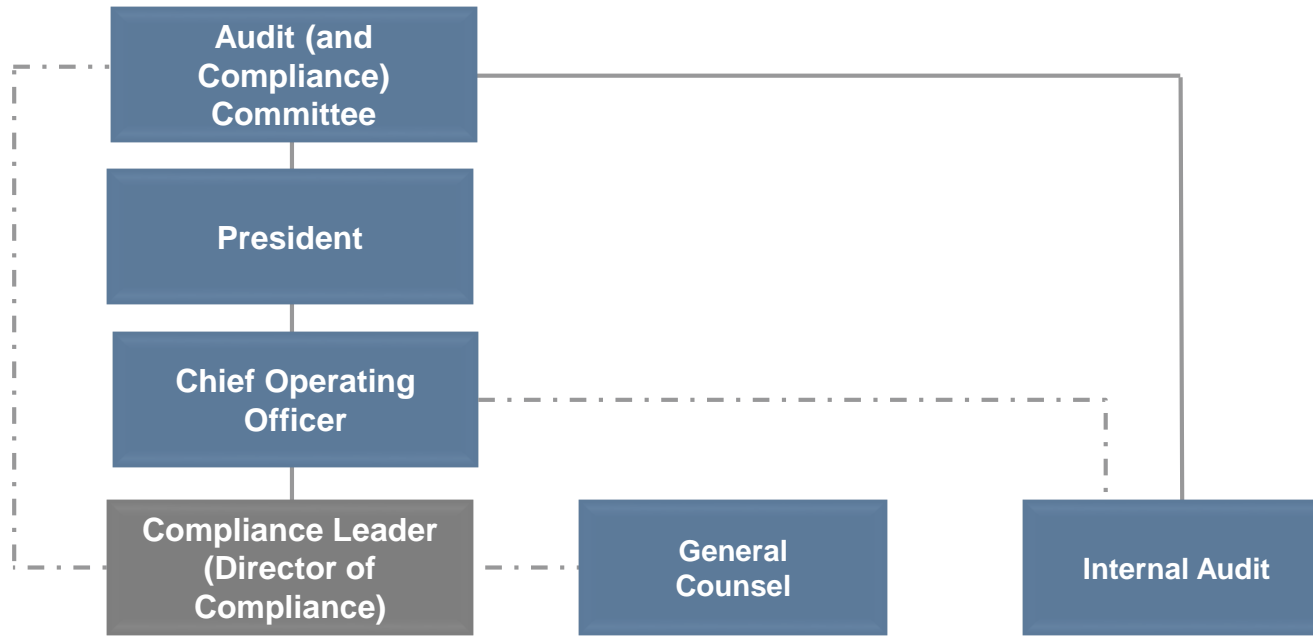
Reporting Lines:

- Dual reporting to Audit (and Compliance) Committee and the President. Direct reporting line to Audit (and Compliance) Committee, 'dotted line' (indirect or administrative) reporting to the President.

- Personnel with responsibilities around compliance will establish a 'dotted line' (indirect) reporting relationship to the Compliance Leader.

- Compliance Leader could be allocated at least one full-time employee to support compliance at a university level.

- Dotted line (Indirect) reporting relationship with General Counsel to establish and maintain Attorney Client Privilege, as necessary.

- Internal Audit has an oversight role and is responsible for independently validating the operating effectiveness of the compliance organization.

Current employee not identified

protiviti®

Future Compliance Organization Structure:
# Option 2 – Director of Compliance Model

Reporting Lines:

- Dual reporting to Audit (and Compliance) Committee and the Chief Operating Officer. Direct reporting line to the Chief Operating Officer, 'dotted line' (indirect or administrative) reporting to the Audit (and Compliance) Committee, as required.

- Personnel with responsibilities around compliance will establish a 'dotted line' (indirect) reporting relationship to the Compliance Leader.

- Compliance Leader could be allocated at least one full-time employee to support compliance at an enterprise level.

- Dotted line (Indirect) reporting relationship with General Counsel to establish and maintain Attorney Client Privilege, as necessary.

- Internal Audit has an oversight role and is responsible for independently validating the operating effectiveness of the compliance organization.

Current employee not identified

protiviti®

University Compliance – Dual Reporting
Option 1 – Direct Reporting

This is a visual representation of an example reporting line structure and is not inclusive of all positions or titles.

protiviti®
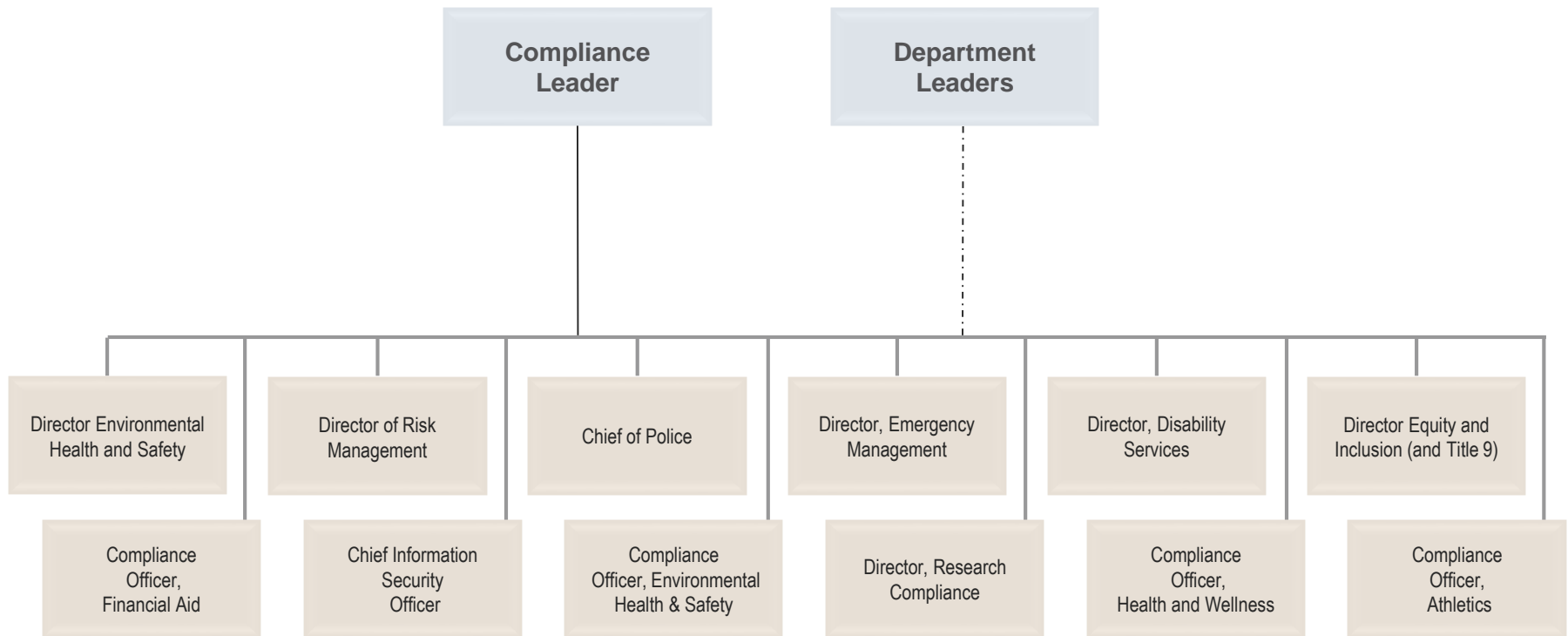
University Compliance – Dual Reporting
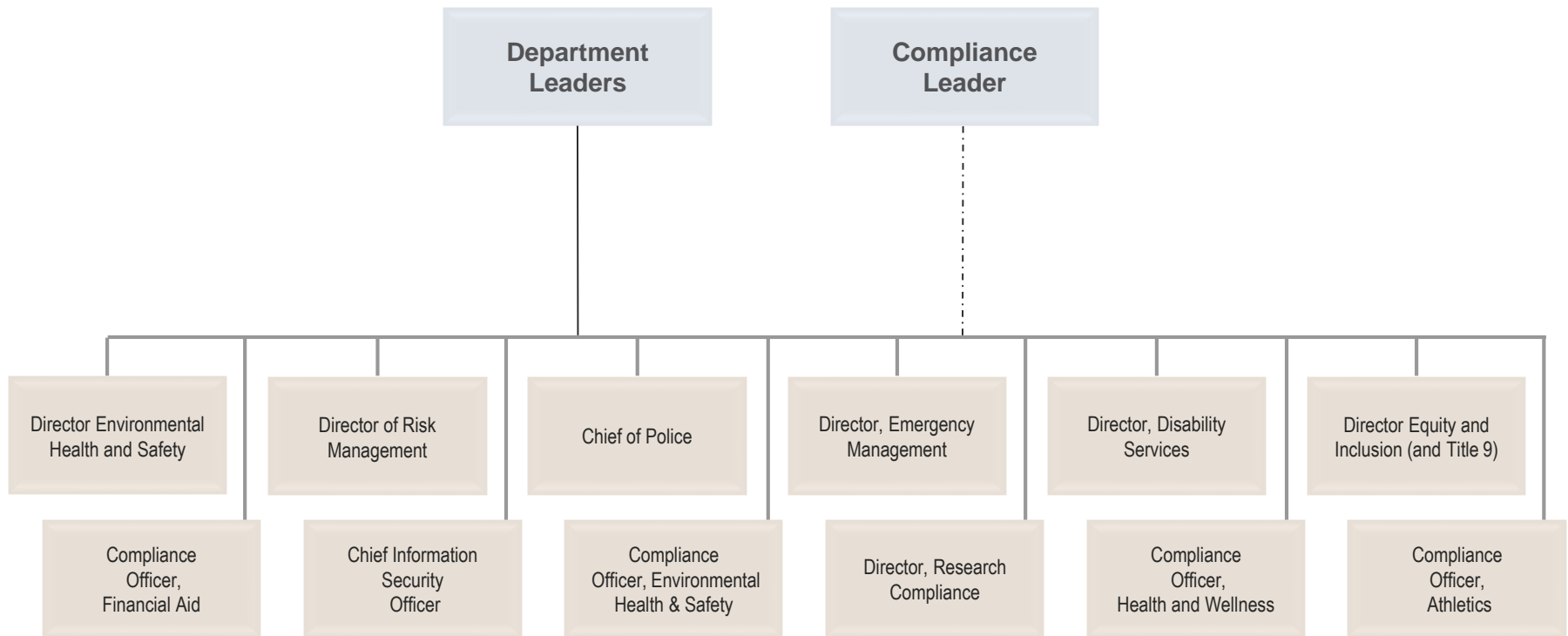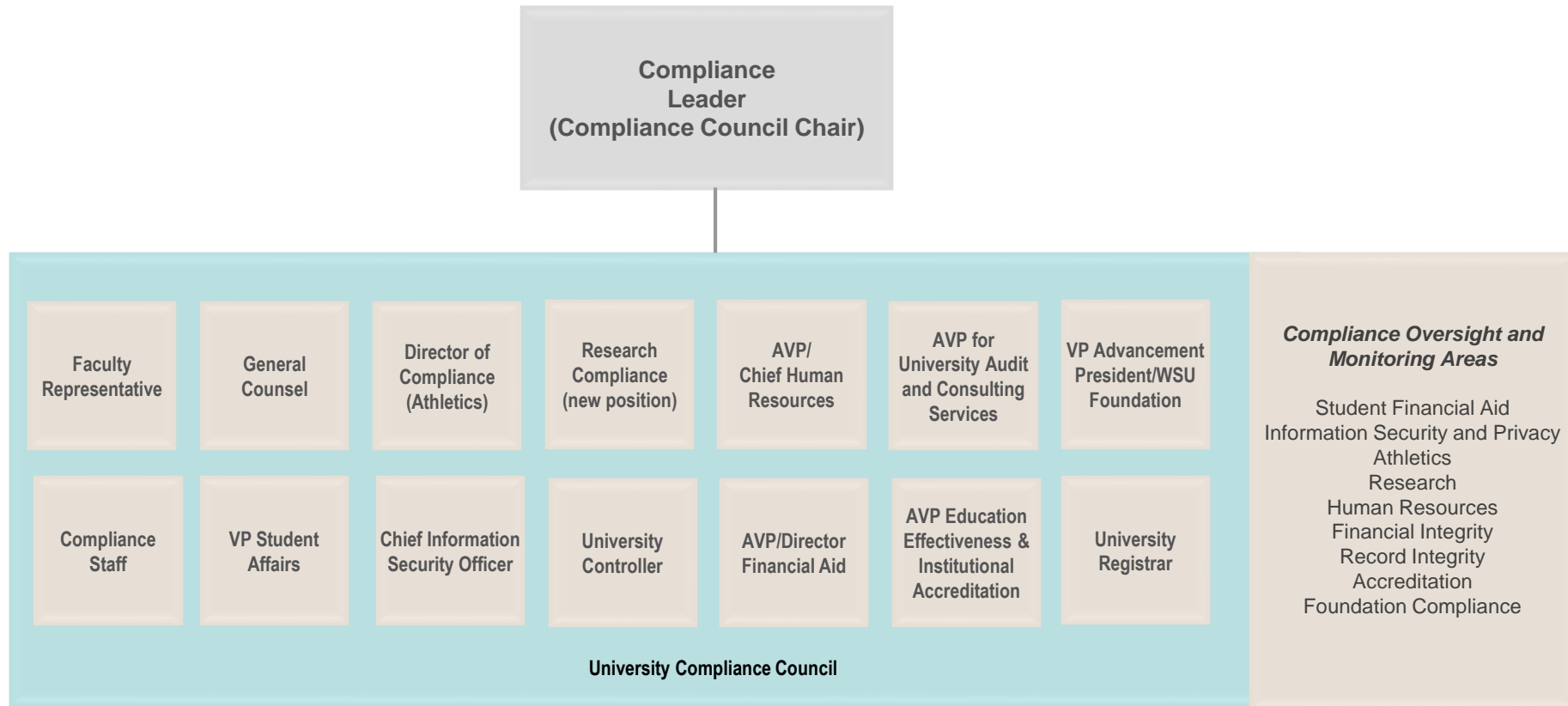# Option 2 – Indirect Reporting

This is a visual representation of an example reporting line structure and is not inclusive of all positions or titles.

protiviti®

University Compliance Council

Compliance
Leader
(Compliance Council Chair)

University Compliance Council

| Faculty Representative | General Counsel | Director of Compliance (Athletics) | Research Compliance (new position) | AVP/ Chief Human Resources | AVP for University Audit and Consulting Services | VP Advancement President/WSU Foundation |
| Compliance Staff | VP Student Affairs | Chief Information Security Officer | University Controller | AVP/Director Financial Aid | AVP Education Effectiveness & Institutional Accreditation | University Registrar |

University Compliance Council

Compliance Oversight and Monitoring Areas

Student Financial Aid
Information Security and Privacy
Athletics
Research
Human Resources
Financial Integrity
Record Integrity
Accreditation
Foundation Compliance

protiviti®

Requirement Identification

Current State Attributes	Key Observations	Recommendations
• Inventories of requirements generally managed informally by department. • Scope and effectiveness of change management practices vary.	• A documented and comprehensive list of compliance requirements within each compliance area generally does not exist. Requirements are generally identified by knowledgeable personnel within each department. • Regional coordination with other State of Ohio institutions is encouraged, especially in highly regulated compliance areas. National participation is limited based on budget and time constraints.	• Create an inventory of compliance requirements for each compliance area.

protiviti®

Requirement Identification – Recommendation Details

- Create an inventory of compliance requirements for each compliance area that includes:

    – All applicable regulatory and contractual requirements.

- Develop method to ensure compliance requirements inventory is maintained / current, including repository tool.

- Inventory manual and system controls in place that promote and enable compliance with requirements identified.

- Identify any compliance control design gaps within each compliance area, assess risk, and remediate.

protiviti®

Risk Assessment

Current State Attributes	Key Observations	Recommendations
• No University-wide risk assessment framework or methodology exists. • Certain Departments perform externally required risk assessments or analyze emerging risks based on external influences.	• No University-wide risk assessment methodology or process exists, most compliance areas do not perform formal or informal risk assessments.	• Identify a comprehensive Compliance Risk Universe. • Develop and implement a university-wide compliance risk assessment.

protiviti®

Risk Assessment – Recommendation Details

- Identify a comprehensive compliance risk universe:
  - Identifies highest risk compliance areas.
  - Identifies Risk Owners.
- Perform a Compliance Risk Assessment (CRA) on an annual basis which:
  - Is led by the new Compliance leader.
  - Includes all significant compliance areas.
  - Evaluate both inherent risk as well as the effectiveness of the controls in place to manage those risks.
  - Leverages any existing risk assessment processes already in place (Internal Audit).
  - Executed by departmental / business line compliance process owners.
  - Is reported to Executive Leadership and the Board of Trustees (or applicable committee).
  - Risk assessment results should be reviewed and updated, as necessary, not less than annually for:
    - ❑ Changes to the business environment.
    - ❑ Changes to laws, regulations, published guidelines.
    - ❑ New information, such as audit and monitoring results and other trends, regarding the effectiveness of the compliance function.
- Create a methodology and process for assessing compliance risk, costs, and benefits related to new business opportunities.

protiviti®

Standards and Controls

Current State Attributes	Key Observations	Recommendations
• Robust, yet inconsistent, Wright Way Policy process. • Other policies, procedures, and guidelines are managed by individual LOBs. • Design of departmental compliance processes vary significantly.	• Policies and procedures are inconsistent across the university. The Wright Way appears to be a good foundation for high level standards and policies, but may not be promoted effectively and is inconsistently updated. • Controls are generally manual and detective in nature.	• Establish a policy governance process to ensure consistency and coordination among policy making groups. (In progress) • Ensure policies and procedures are reviewed on a regular basis to ensure they are accurate and up to date. • Based on risk assessment results, identify related key controls and increase preventative controls for key areas, where possible. • Consider enhancing the Institution-wide Ethics Policy to become a more comprehensive Code of Conduct addressing key issues such as compliance program governance, non-retaliation, and how to report concerns anonymously or confidentially.

protiviti®

Standards and Controls – Recommendation Details

- Leverage and further enhance the Wright Way policy structure and establish a Compliance Policy which, at minimum, outlines:

    - Definition of compliance.

    - Roles and responsibilities of key stakeholders.

- Consider developing a "Policy on Policies": (in progress)

    - Outlines the process for developing new policies.

    - Outlines approval process for policies / procedures.

- Create an inventory of all university policies and procedures that promote compliance, and a process to periodically revise for accuracy:

    - Use cross functional teams to review policies, when appropriate.

    - Final approved policies should be published on a centralized website to be administered by the University Compliance Office.

    - University Compliance Office should establish a uniform hierarchy and standard templates for procedures, guidelines, and other process documentation; these requirements could be documented in the Policy on Policies or a similar complementary standards document.

protiviti®

Code of Conduct – Recommendation Details

- Leverage the current Wright Way Ethics Policy to create an institution-wide Code of Conduct (the Code) applicable to all trustees, faculty and administration members, employees, students, suppliers and other parties responsible for maintaining the integrity of the institution.

- Incorporate Wright's Dispute Resolution Procedures on non-retaliation within the Code of Conduct.

- Document the Board's expectation that all University stakeholders will act ethically, with integrity and in a manner that preserves the values and reputations of the Institution (tone at the top).

- The Code shall be consistent with and support the mission and values of the University.

- Take into account the University's unique culture and the views of all stakeholder groups.

- Assign accountability for implementing and maintaining the policies and processes that relate to the Code.

- Code of Conduct should address key issues such as:

    - Compliance program governance.

    - Non-retaliation.

    - Types of issues that should be reported and the concepts of "good faith" reporting.

    - How to report concerns anonymously or confidentially.

protiviti®

Training

Current State Attributes	Key Observations	Recommendations
• Training generally managed by individual Departments. • No unified training delivery platform or University-level tracking of compliance.	• Training mechanisms and tools vary across the University. There are multiple training delivery and tracking tools in the various departments and there may be opportunities to leverage and centralize to promote consistency and cost effectiveness. • Required training is considered mandatory, but is not enforced on a regular or consistent basis.	• Establish a consistent methodology to identify compliance training needs of faculty, administrators, employees, students and other stakeholders. • Develop an annual compliance training plan based on the compliance risk assessment. • Ensure training is documented and tracked to completion.

protiviti®

Training – Recommendation Details

- Develop and document an annual and on-going compliance training plan based on the compliance risk assessment to address specific risk areas.

- Tracking Training:

  - Consider leveraging one of the existing software tools to house / deliver / track all training content. Metrics should be used to ensure trainings are consistent with university goals.

  - University Compliance Office could collaborate with HR to enforce accountability, especially for mandatory compliance related trainings.

  - System should support manual uploads of sign-in sheets or comparable documentation of training performed offline in order to enable a complete view of the training received by each individual, regardless of source.

  - Develop reporting and escalation procedures to ensure mandatory compliance training is completed.

protiviti®

Monitoring and Remediation

Current State Attributes	Key Observations	Recommendations
• Most Departments are doing some proactive quality assurance, but do not have effective monitoring processes in place. • Remediation activities are mainly based on external findings.	• Compliance monitoring is generally restricted to required audits by external sources, but are generally welcomed as opportunities for change. • Select highly regulated areas have consistent monitoring; however within other areas, if monitoring exists, is performed as time allows or as issues are identified. • No centralized tracking or follow-up of known compliance risks and findings/issues exists. • Internal audit does not appear to include sufficient compliance objectives in their audits to provide adequate monitoring control for the University.	• University Compliance Office should be charged with ensuring key compliance risks to the University are subject to consistent and comprehensive monitoring. • Consider "Three lines of Defense" approach. • Develop a risk, finding, and remediation tracking system to ensure appropriate follow-up and management of these matters. • Clarify Internal Audit's role in compliance monitoring.

protiviti®

Monitoring and Remediation – Three Lines of Defense

- Establish and communicate roles in "Three lines of defense" monitoring approach:

    1. Business / Operational management / process owners

    2. Compliance / risk management functions

    3. Internal Audit

The Three Lines of Defense Model

Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

protiviti®

Monitoring and Remediation – Recommendation Details

- Establish a process for risk-based compliance monitoring to evaluate whether compliance objectives are being met. This process should be owned by the Compliance function.

  - Track compliance gaps (i.e., issues log) and status of remediation for non-compliance issues to enable prompt resolution and accountability.

  - Define a process for periodically reporting compliance status, issues, and resolution to senior management / Board of Trustees.

- Monitoring of compliance by University Compliance Office responsibilities include:

  - Identifying risks that require remediation or monitoring activities based on the compliance risk assessment results or other trends and analysis

  - Collaboratively working with compliance personnel to design remediation or monitoring plans.

  - Ensuring the timely execution of remediation or monitoring procedures are performed by compliance personnel.

  - Performing follow up reviews to ensure that high risk control gaps have been closed.

protiviti®

Suggested Implementation Approach

A phased implementation approach is recommended and illustrated below. It is recommended the University prioritize hiring a Compliance Leader to guide the University through establishing a University Compliance function and formalizing the remaining compliance infrastructure elements.

Phases	Phase I: Org Structure, Standards and Controls	Phase II: Requirement Identification, Monitoring and Remediation	Phase III: Risk Assessment, On-Going Compliance Training
Activities	• Hire a Compliance Leader (Chief Compliance Officer/Director) • Create a compliance strategy and policy • Define key processes which require compliance involvement • Set owners for each compliance area • Establish a Compliance Council • Formalize the process for identifying new compliance requirements • Educate employees on new compliance function and structure	• Inventory all organization-wide compliance requirements • Inventory controls in place, identify and remediate gaps, and define new controls as-needed • Define a process for reporting compliance status to Executives / Board of Trustees • Establish a process for risk-based compliance monitoring • Educate employees on compliance requirements • Create compliance document repository	• Perform a compliance risk assessment • Create a process for assessing compliance risk and costs for new business opportunities • Develop an integrated and continuous compliance training program
Outcomes	• Accountability for compliance is defined, communicated, and understood • Compliance policies are in place • Compliance becomes integrated within business processes	• Universe of compliance requirements is documented and controls identified to mitigate risk • Compliance control gaps are identified and remediated • Employees are aware of compliance requirements	• On-going compliance training is provided to employees • Management understands and controls the highest risk compliance areas

protiviti®

Appendices

Appendix A – Protiviti Compliance Framework (PCF)

- ❑ Compliance is a constantly-evolving lifecycle, rather than a process with a single endpoint. With many touch points throughout an organization, the PCF is a flexible framework that enables a holistic view of compliance across an organization.

- ❑ The PCF provides a roadmap to evaluate the effectiveness of a compliance program and incorporates published guidelines from a wide variety of sources, including:

  - ✓ Federal and international standards issued for the banking, financial services, healthcare, and other industries

  - ✓ US Federal judiciary standards

  - ✓ Protiviti's experience working with clients

Manage Regulatory Exams

Audit the Effectiveness of the Program

Adjust the Program as Necessary

Remediate Compliance Deficiencies

Requirement Identification

Risk Assessment

Standards and Controls

Training

Monitoring and Remediation

Organizational Structure and Accountability

EVALUATE · IDENTIFY · ASSESS · EXECUTE

Board and Senior Management Involvement

protiviti®

Appendix B – Sample RACI Assignments – Future

Selected Future State Compliance Processes - Proposed Owners	Line of Business Compliance Personnel	Department Leadership	Office of Institutional Compliance Personnel	Chief Compliance Officer	Institutional Compliance Committee	Chief Operating Officer / Provost	General Counsel	Significant Incident Group	Senior Staff	Finance Committee of the BOT	Board of Trustees
Compliance Risk Assessment											
Designing and implementing risk assessment methodology	I	I	C	A/R	C	C	I		I	C	I
Executing initial and periodically updating risk assessment results	R	C	C	A	C	C	I		I	I	I
Policies and Procedures											
Developing Code of Conduct	I	I	R	A	R	C	C		C	C	C
Creating and updating policies	R	C	R	A	C	C	C		C	C	I
Creating and updating procedures	A	C	C	C	I	C	C				
Change Management											
Evaluating and approving compliance risks and controls related to proposed change activities (normal course)	R	C	R	C	A	C	C				
Evaluating and approving compliance risks and controls related to proposed change activities (escalations)	C	R	C	C	R	C	C		A	I	
Compliance Training Program											
Performing initial and annual training needs assessment.	R	C	C	A	C	C	C		I	I	
Monitoring and Investigations											
Performing regularly-scheduled monitoring procedures.	R	I	R	A	C	C	C		I	I	I
Conducting ad hoc monitoring reviews in response to emerging issues.	I	I	R	A	C	C	C		I	I	I
Conducting special investigations (e.g., in response to complaints)	R	I	R	R		C	A	C	I	C	I

Legend:	
	R - Responsible (Those who do the work to achieve the task. There can be multiple resources responsible.)
	A - Accountable / Approver (The resource ultimately answerable for the correct / thorough completion of the task. Can't be delegated.)
	C - Consulted (Those whose opinions are sought. Two way communication.)
	I - Informed (Those who are kept up-to-date on progress. One way communication.)

protiviti®

Powerful Insights.
Proven Delivery.™