BOARD OF REGENTS OF THE UNIVERSITY OF WISCONSIN SYSTEM

Audit Committee

Via WebEx Videoconference

Thursday, October 8, 2020
8:45 a.m. – 10:00 a.m.

A. Calling of the Roll

B. Declaration of Conflicts

C. Approval of the Minutes of the August 20, 2020 Meeting of the Audit Committee

D. State of Wisconsin Legislative Audit Bureau

    1. Beginning of Audit Letter for the June 30, 2020 UW System Financial Statements Audit

E. Internal Audit
    1. Fiscal Year 2021 Audit Plan Progress Report
    2. Summarized Results of Audits Recently Issued

F. Compliance
    1. Update on the office of Compliance and Integrity restructuring
    2. Youth Protection and Compliance Update

Audit Committee **Item D.1.**
October 8, 2020

Beginning of Audit Letter for the June 30, 2020 UW System Financial Statements Audit

REQUESTED ACTION

Item for information and discussion only.

SUMMARY

As directed by s.13.94(1) (t), Wis. Stats., the Legislative Audit Bureau (LAB) will conduct a financial audit of UW Systems' financial statements, which include the related notes as of and for the year ended June 30, 2020. The LAB is also performing the State of Wisconsin's FY 2019-20 single audit which will include work at UW System. LAB will communicate their responsibilities under generally accepted auditing standards.

Presenter(s)

- Erin Scharlau, Financial Audit Director, LAB

Attachments

A) Legislative Audit Bureau Beginning of Audit Letter

STATE OF WISCONSIN | Legislative Audit Bureau

22 East Mifflin St., Suite 500 ▪ Madison, WI 53703 ▪ (608) 266-2818 ▪ Hotline: 1-877-FRAUD-17 ▪ www.legis.wisconsin.gov/lab

Joe Chrisman
State Auditor

August 19, 2020

Mr. Andrew Petersen, President and
Members of the Audit Committee of the Board of Regents
University of Wisconsin System
1860 Van Hise Hall
1220 Linden Drive
Madison, Wisconsin 53706

Dear President Petersen and Members of the Audit Committee of the Board of Regents:

This letter communicates information and responsibilities regarding two audits the Legislative Audit Bureau will perform of the University of Wisconsin (UW) System. As directed by s. 13.94(1) (t), Wis. Stats., the Audit Bureau will conduct a financial audit of UW System. This includes auditing UW System's financial statements, which include the related notes, as of and for the year ended June 30, 2020. The financial statements and related notes will be included in UW System's annual financial report.

Second, the Legislative Audit Bureau is performing the State of Wisconsin's FY 2019-20 single audit, which is a comprehensive audit of state government to meet the State's needs and audit requirements established by the federal Office of Management and Budget *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance), the Single Audit Act of 1984, and the Single Audit Act Amendments of 1996. This includes auditing the basic financial statements, which include the related notes, for the State of Wisconsin as of and for the year ended June 30, 2020, as included in the State of Wisconsin's Comprehensive Annual Financial Report, as well as federal financial assistance expended by the State of Wisconsin. The single audit will include work at UW System.

In performing this audit, we will follow generally accepted auditing standards issued by the American Institute of Certified Public Accountants and *Government Auditing Standards,* which is issued by the Comptroller General of the United States. These standards require us to agree upon, with the audited entity, the terms of this engagement, including auditor and management responsibilities. While this document is a matter of public record, it is intended solely for the information and use of the President of the Board of Regents and the Audit Committee of the Board of Regents, and UW System's management and is not intended to be and should not be used by anyone other than these specified parties.

Legislative Audit Bureau

The Bureau supports the Legislature in its oversight of Wisconsin government and its promotion of efficient and effective state operations by providing nonpartisan, independent, accurate, and timely audits and evaluations of public finances and the management of public programs. Because the Bureau is a legislative service agency, the audit results, including recommendations for improvements in agency operations, are reported to the Legislature. Following the release of the reports, the Joint Legislative Audit Committee may choose to hold a public hearing on the reports.

Audit Scope and Objective

Financial Audit of UW System

An objective of our audit of UW System is the expression of an opinion on whether the financial statements included in UW System's annual financial report that have been prepared by management with the oversight of the President of the Board of Regents and the Audit Committee of the Board of Regents, are fairly presented, in all material respects, in conformity with accounting principles generally accepted in the United States of America. Generally accepted auditing standards require that we obtain reasonable assurance about whether the financial statements are free from material misstatement.

We are not responsible for auditing or expressing an opinion on required supplementary information included in the report that is presented for purposes of additional analysis and is not a required part of the financial statements, but is required by accounting principles generally accepted in the United States of America. Such information includes the Management's Discussion and Analysis and schedules related to UW System's proportionate share of the net pension liability (asset), pension contributions, UW System's proportionate share of the net other post-employment benefits (OPEB) liability (asset), and OPEB contributions. We are not responsible for auditing or expressing an opinion on supplementary or other information included in the report that is presented for purposes of additional analysis and is not a required part of the financial statements.

Our audit will also provide a report on UW System's internal control over financial reporting and its compliance with certain provisions of laws, regulations, contracts and grant agreements that could have a material effect on the financial statements. This report includes deficiencies in internal control considered to be significant deficiencies or material weaknesses, instances of fraud and noncompliance that have a material effect on the financial statements, and fraud that is material, either quantitatively or qualitatively, to the financial statements. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the UW System's internal control over financial reporting and compliance. The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of internal control or on compliance. Accordingly, this report is not suitable for any other purpose.

Statewide Single Audit

UW System Financial Statements in the State of Wisconsin's Comprehensive Annual Financial Report—An objective of our audit is the expression of an opinion on whether the State of Wisconsin's

basic financial statements that have been prepared by the Department of Administration, State Controller's Office based upon information submitted by state agencies, including UW System, and with the oversight of the Secretary of the Department of Administration and the State Controller, are fairly presented, in all material respects, in conformity with accounting principles generally accepted in the United States of America. Generally accepted auditing standards require that we obtain reasonable assurance about whether the financial statements are free from material misstatement.

Our audit will also provide an opinion on whether the combining statements and schedules are fairly presented in relation to the basic financial statements taken as a whole. We are not responsible for auditing or expressing an opinion on required supplementary information, other supplementary information, or information included in the report that is presented for purposes of additional analysis and is not a required part of the financial statements, but is required by accounting principles generally accepted in the United States of America. An example of required supplementary information is management's discussion and analysis.

In addition, we will provide a report on the State's internal control over financial reporting and its compliance with certain provisions of laws, regulations, contracts and grant agreements that could have a material effect on the financial statements. This report includes deficiencies in internal control considered to be significant deficiencies or material weaknesses, instances of fraud and noncompliance that have a material effect on the financial statements, and fraud that is material, either quantitatively or qualitatively, to the financial statements. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the State's internal control over financial reporting and compliance. The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of internal control or on compliance. Accordingly, this report is not suitable for any other purpose.

Federal Compliance Audit—An objective of our audit is the expression of an opinion on the State's compliance with federal rules and regulations for its major federal programs. Generally accepted auditing standards require that we obtain reasonable assurance about whether the State of Wisconsin complied with program requirements for major federal programs. Our audit will also provide an opinion on whether the Schedule of Expenditures of Federal Awards is fairly presented in relation to the basic financial statements taken as a whole.

In addition, we will provide a report on the State's internal control over compliance with major federal program requirements and provisions of certain laws, regulations, contracts, and grant agreements that could have a material effect on a major federal program. This report includes deficiencies in internal control considered to be significant deficiencies or material weaknesses, instances of fraud and noncompliance that have a material effect on a major program, and fraud that is material, either quantitatively or qualitatively, to a major program. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the State's internal control over compliance. The purpose of this report is solely to describe the scope of our testing of internal control over compliance and the results of this testing, and not to provide an opinion on the effectiveness of internal control over compliance. Accordingly, this report is not suitable for any other purpose.

Audit Procedures

We will plan and perform these audits to obtain reasonable assurance about whether the financial statements are free from material misstatement and whether the State materially complied with federal grant program requirements for each major program. The procedures selected will depend on the auditor's judgment, including the assessment of the risks of material misstatement.

Financial Audit of UW System

This audit will include obtaining an understanding of the UW System and its environment, including its internal control that is sufficient to assess the risks of material misstatement of the financial statements and to design the nature, timing, and extent of further audit procedures. Our audit will also include evaluating the appropriateness of the accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

As noted, our audit is not designed to express an opinion on internal control over financial reporting. If, during the audit, we become aware of any such deficiencies considered to be significant deficiencies or material weaknesses, we are responsible for communicating them to the UW System management, the President of the Board of Regents, and the Audit Committee of the Board of Regents, along with communicating any other matters identified during our audit that are relevant to their responsibilities in overseeing the financial reporting process. However, auditing standards do not require us to design our procedures solely for the purpose of identifying other matters to communicate. Further, our responsibility as auditors is limited to the period covered by our audit and does not extend to any other periods for which we were not engaged as auditors.

We will also apply certain limited procedures to ensure supplementary and other information, or the manner of its presentation, is materially consistent with the financial statements. At the conclusion of the audit, we will also request that the UW System's management provide us with a letter that confirms certain representations made during the audit. In addition, we may request written representations from the UW System's attorney as part of the engagement.

UW System's financial statements include significant financial information related to capital accounting and debt, which is provided by the Wisconsin Department of Administration. Another audit team of the Audit Bureau performs a separate audit of the information provided by the Department of Administration. We coordinate our audit work with the work completed by this audit team, and, ultimately, we rely upon the work of this audit team as part of our audit of UW System. Therefore, the timing of completion of audit fieldwork and issuance of our audit opinion is dependent, in part, on the availability of the information provided by the Department of Administration.

In addition, UW System's annual financial report will include the financial statements of the UW Foundation and the UW-Milwaukee Foundation. We intend to rely on the audit work performed by external auditors engaged by the UW Foundation and the UW-Milwaukee Foundation to perform separate financial statement audits. We do not plan to perform audit work related to this financial information and instead will make reference to the work of these

external auditors in our auditor's report. We will inform the external auditors of our intent and will also perform some limited procedures to verify that the audited financial information has been appropriately included in UW System's annual financial report. We will also communicate with the external auditors to obtain any information necessary for us to rely on their work, such as certain representations related to their work. Therefore, the timing of completion of audit fieldwork and issuance of our audit opinion is dependent, in part, on the completion of the financial statement audits of the UW Foundation and UW-Milwaukee Foundation and receipt of necessary information from the external auditors. In 2019, this type of audit evidence was made available to the Audit Bureau as part of our audit of the State's Comprehensive Annual Financial Report on December 11, 2019.

Statewide Single Audit

UW System Financial Statements in the State of Wisconsin's Comprehensive Annual Financial Report—This audit will include a review of UW System's financial statements and related disclosures as presented in the State of Wisconsin's Comprehensive Annual Financial Report for fiscal year 2019-20. The Audit Bureau will request UW System's management provide a letter that confirms certain representations related to the presentation of UW System's financial statements in the State of Wisconsin's Comprehensive Annual Financial Report. In addition, any deficiencies in internal control, instances of fraud, or noncompliance identified during our audit of the UW System's financial statements may be required to be reported to the Secretary of the Department of Administration and the State Controller.

Federal Compliance Audit—This audit will include obtaining an understanding of internal control over compliance with requirements that could have a direct and material effect on a major program sufficient to plan the audit to support a low level of control risk and to determine auditing procedures for the purposes of expressing an opinion on compliance and to test and report on internal control over compliance in accordance with the Uniform Guidance. Major programs are determined using the risk-based approach required by Uniform Guidance. For the fiscal year 2019-20 audit, we have selected the Research and Development Cluster and the Education Stabilization Fund. Audit work will be performed at select UW institutions. In addition, we will perform follow-up work related to finding 2018-700.

At the conclusion of the audit, we will request that UW System's management provide us with a letter that confirms certain representations made during the audit related to compliance with federal grant program requirements.

The inherent limitations of an audit, together with the inherent limitations of internal control, result in an unavoidable risk that some material misstatements may not be detected, even though the audit is properly planned and performed in accordance with generally accepted auditing standards and *Government Auditing Standards.* In addition, an audit is not designed to detect misstatements, fraud, or violations of provisions of applicable laws, regulations, contracts, and grant agreements that do not have a material effect on the financial statements. We will inform UW System management, the President of the Board of Regents, and the Audit Committee of the Board of Regents of any fraud or violations of provisions of applicable laws, regulations, contracts, and grant agreements that come to our attention, unless clearly inconsequential. We cannot provide assurance that an unmodified opinion will be expressed. Circumstances may arise in which it is necessary for us to modify our opinion or add emphasis-of-matter or

other-matter paragraphs. If, for any reason, we are unable to complete the audit or are unable to form an opinion, we may decline to express an opinion or decline to issue a report as a result of the engagement.

Although generally accepted auditing standards and *Government Auditing Standards* require that we communicate certain matters to the management of UW System, the President of the Board of Regents, and the Audit Committee of the Board of Regents, s. 13.94, Wis. Stats., requires that an audit remain confidential until it is released. In accordance, we will complete certain audit procedures, such as draft audit-related communications, only through interactions with UW System management.

Management's Responsibilities

UW System is responsible for:

- the design, implementation, and maintenance of effective internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to error or fraud;

- the selection and application of accounting principles;

- the preparation and fair presentation of the financial statements, related notes, and required supplementary information included in UW System's annual financial report in accordance with accounting principles generally accepted in the United States of America;

- the preparation and fair presentation of other supplementary information contained in UW System's annual financial report;

- the preparation and fair presentation of the financial statements, related notes, required supplementary information, and other information submitted to the State Controller's Office for inclusion in the State of Wisconsin's Comprehensive Annual Financial Report in accordance with accounting principles generally accepted in the United States of America and the Uniform GAAP Conversion Policies and Procedures Manual, which is prepared by the State Controller's Office;

- the preparation and fair presentation of other supplementary information submitted to the State Controller's Office for inclusion in the State of Wisconsin's Comprehensive Annual Financial Report;

- the identification of federal programs and the understanding of applicable compliance requirements;

- compliance with provisions of applicable laws, regulations, contracts, and grant agreements, including evaluating and monitoring compliance;

- the design, implementation, and maintenance of effective internal control relevant to compliance with federal rules and regulations;

- the preparation and fair presentation of information submitted to the State Controller's Office for inclusion in the State of Wisconsin's Schedule of Expenditures of Federal Awards in accordance with Uniform Guidance requirements;

- following up and taking timely corrective action on audit findings and other instances of noncompliance, including preparation of a corrective action plan for findings, and submission of the corrective action plan on letterhead to the Legislative Audit Bureau; and

- the preparation and submission of the status of prior audit findings, if any, on agency letterhead to the Legislative Audit Bureau for inclusion in the Summary Schedule of Prior Audit Findings.

UW System is responsible for the accuracy and completeness of all financial records and related information, and providing certain representations at the conclusion of the audit. These responsibilities also include adjusting the financial statements to correct material misstatements and affirming to us in the management representation letter that the effects of uncorrected misstatements aggregated by us during the current engagement and pertaining to the latest period presented are immaterial, both individually and in the aggregate, to the financial statements taken as a whole.

UW System will provide access to all information of which it is aware that is relevant to the preparation and fair presentation of the financial statements, such as records and documentation. UW System will also provide additional information that the Bureau may request from UW System for the purpose of the audit and unrestricted access to persons within UW System from whom the Audit Bureau determines it necessary to obtain audit evidence. UW System will provide financial statements, related notes, and any supplementary and other information in a timely manner and will provide reasonable assistance in collecting necessary financial information and performing other tasks.

UW System is responsible for the design and implementation of programs and controls to prevent and detect fraud and for informing us about all known or suspected fraud involving (a) management, (b) employees who have significant roles in internal control, and (c) others where the fraud could have a material effect on the financial statements. In addition, UW System is responsible for identifying and ensuring that it complies with provisions of applicable laws, regulations, contracts, and grant agreements.

UW System will include the auditor's opinion in any paper or electronic publication of the UW System's financial statements. UW System will contact the Audit Bureau if it intends to produce an electronic or paper publication of the financial statements that is separate from the State of Wisconsin's Comprehensive Annual Financial Report or UW System Annual Financial Report that indicates that the Audit Bureau has reported on such information.

Our audits do not relieve UW System management, the President of the Board of Regents, or the Audit Committee of the Board of Regents of its responsibilities.

Administrative Matters

The audit workpapers for this engagement remain confidential until we release the auditor's reports. At that time, statutes provide that they become open records unless they are otherwise confidential by law, in which case they will remain confidential. Upon completion of the audit and issuance of the audit report, the audit workpapers will be made available for examination at the Audit Bureau's office at any reasonable time. Audit workpapers and reports will be maintained for a minimum of seven years from the date of the audit's release.

The Audit Bureau participates in a peer review program with other state auditing organizations covering our audit practices. This program requires that we subject our system of quality control to an examination by a peer review team once every three years. As part of the process, the peer review team will review a sample of our work, some of which may include confidential information.

We have already begun our audit fieldwork. We will keep management informed of the time frame for releasing our audit opinion on the financial statements and our report on internal control and compliance.

We look forward to working with UW System to complete our audit work and believe this letter summarizes the significant terms of our engagement. If you have any further questions related to the audit, please feel free to contact me at 266-2818.

Sincerely,

Erin Scharlau

Erin Scharlau
Financial Audit Director

ES/DS/km

cc: Tommy Thompson, Interim President
University of Wisconsin System

Sean Nelson, Vice President for Finance
University of Wisconsin System

Robert Cramer, Vice President for Administration
University of Wisconsin System

Julie Gordon, Senior Associate Vice President for Finance
University of Wisconsin System

Lori Stortz, Chief Audit Executive
University of Wisconsin System

Audit Committee **Item E.1.**
October 8, 2020

FISCAL YEAR 2021 AUDIT PLAN PROGRESS

REQUESTED ACTION

For information and discussion only.

SUMMARY

One of the responsibilities of the Audit Committee, as outlined in the committee charter, is to review and approve the annual internal audit plan and receive interim progress reports at least quarterly.

The attached chart provides a summary of audit progress for the Fiscal Year 2021 Audit Plan.

Presenter(s)

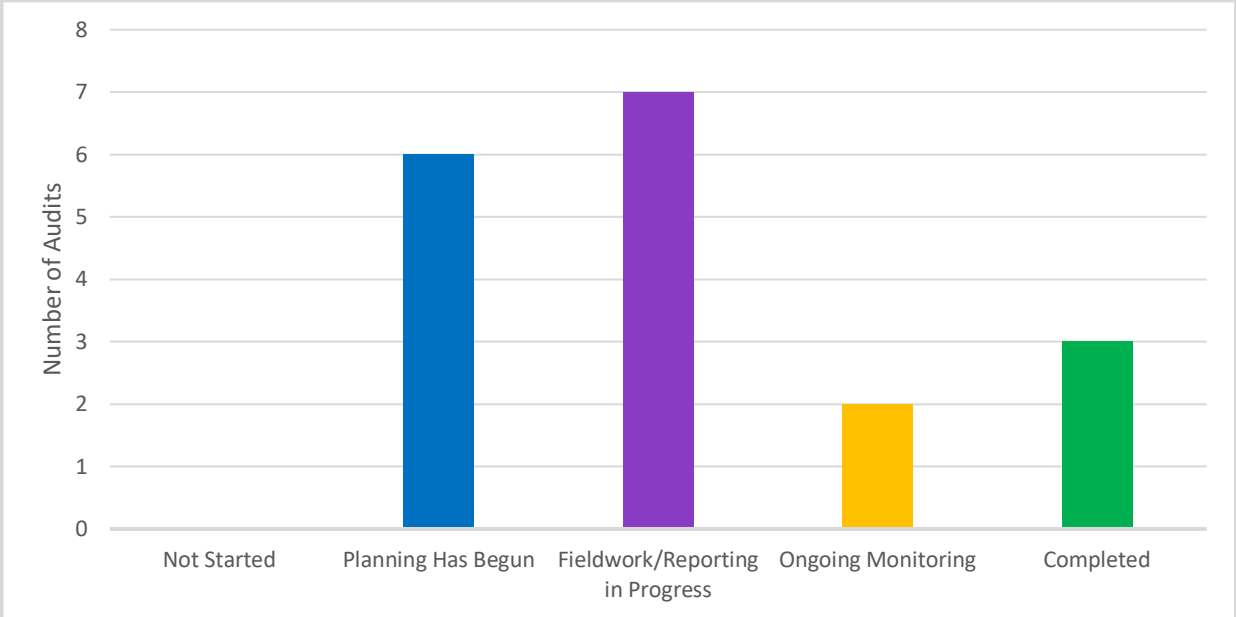
- Lori Stortz, Chief Audit Executive

ATTACHMENTS

A) UW System Administration Office of Internal Audit Fiscal Year 2021 Audit Plan Progress Chart.

UW SYSTEM ADMINISTRATION
OFFICE OF INTERNAL AUDIT
FISCAL YEAR 2021
AUDIT PLAN PROGRESS

	Title	Risks
1	Payroll (Continuous Monitoring)	Fraud
2	Purchasing Cards (Continuous Monitoring)	Fraud, Embezzlement
3	Post-Tenure Review	Compliance with Board Policy
4	Oversight of Programs with Minors	Physical Safety and Security
5	Other Affiliated Organizations	Fraud, Embezzlement, Reputation
6	Laboratory Safety	Physical Security and Safety, Legal Compliance
7	Emergency Grant Aid Payments to Students Under the CARES Act	Regulatory Compliance, Reputation
8	Information Technology Disaster Recovery	Continuity of Operations, Data Protection
9	Incident Response	Data Availability, Breach of Information, Reputation
10	Security Awareness	Data Security, Reputation
11	Foreign Influence	Regulatory Compliance, Reputation
12	Contracts with Private Entities	Conflict of Interest, Reputation
13	NCAA Division III Athletics Financial Transactions	Fraud, Conflicts of Interest, Reputation
14	Independent Contractors	Fraud, Regulatory Compliance, Conflict of Interest
15	Change Requests of Bank and Contact Information	Fraud
16	Non-Competitive Bids	Fraud, Regulatory Compliance, Conflicts of Interest
17	NCAA Athletics Division I Consulting Engagements	Data Accuracy
18	Internal Assessment	Conformance with Standards, Code of Ethics



SUMMARIZED RESULTS OF AUDITS RECENTLY ISSUED

REQUESTED ACTION

For information and discussion only.

SUMMARY

Since the August 20, 2020 meeting of the Audit Committee, the Office of Internal Audit has issued the following reports:

- Internal Audit Responses to Independent Validation
- Laboratory Safety Best Practices Report
- Laboratory Safety Executive Summary
- Pcard Continuous Audit
- Payroll Continuous Audit

Presenter(s)

- Lori Stortz, Chief Audit Executive

BACKGROUND

One of the responsibilities of the Audit Committee, as outlined in the committee charter, is to summarize results of audits recently issued.

Audit Committee **Item F.1.**
October 8, 2020

UPDATE ON THE OFFICE OF COMPLIANCE AND INTEGRITY RESTRUCTURING

REQUESTED ACTION

Item for information and discussion only.

SUMMARY

In February 2019, the Office of Compliance and Integrity was created within the Office of General Counsel. The Director of Compliance, Katie Ignatowski, reported directly to the General Counsel for the UW System. Effective September 15, 2020, the Office of Compliance and Integrity moved to a direct reporting line to the President of the UW System as shown in Attachment A and the Director's title was renamed to Chief Compliance Officer. This move is consistent with national trends and best practices in both institutions of higher education and in private industry as referenced on page 7 in Attachment B, pages 10-11 in Attachment C , and page 7 in Attachment D. The plan to restructure the Office of Compliance and Integrity also includes a proposal to work with the Audit Committee of the Board of Regents to pursue the adoption of a dual reporting line from the Chief Compliance Officer to the Chair of the Audit Committee, similar to the reporting structure for the Chief Audit Executive. This proposal would be developed in collaboration with the Chief Audit Executive, UW System leadership and campus leadership over the next 6-9 months and be brought back before the Committee in 2021. This update will also include an overview of new compliance issue areas for which the Office of Compliance has assumed responsibility over the past two months.

Presenter(s)

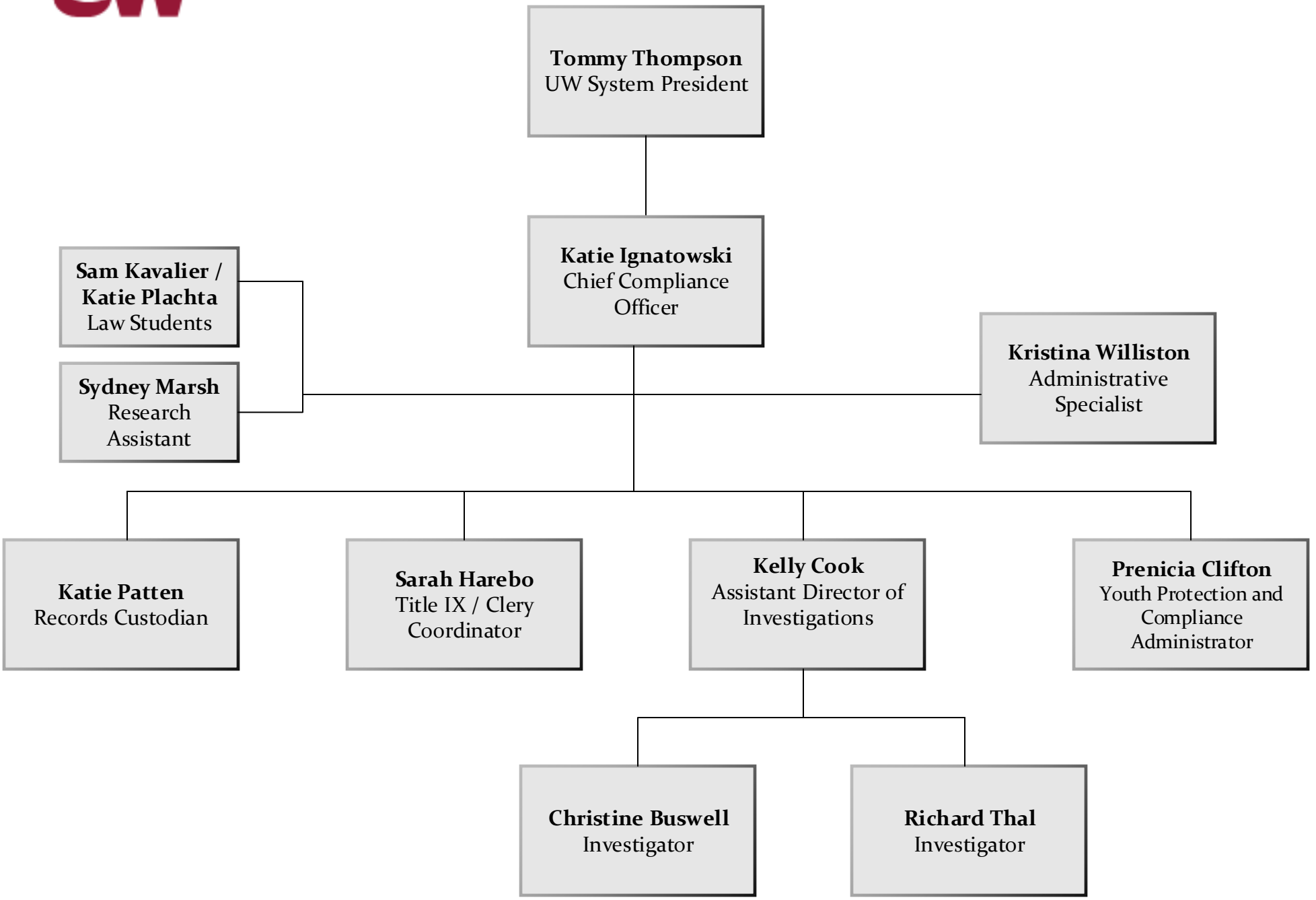
- Katie Ignatowski, Chief Compliance Officer, UW System Office of Compliance and Integrity

Attachments

A) Organizational Chart
B) 2018 NACUA Compliance Survey Results
C) USDOJ Evaluation of Corporate Compliance Programs
D) Institute for Internal Auditors Three Lines of Defense Model

University of Wisconsin System

Office Of Compliance and Integrity



NACUA

2018 Annual Conference

Hilton Minneapolis · Minneapolis, MN
June 24 – 27, 2018

09I

The Results of NACUA's 2018 Compliance Survey

SUMMARY OF RESULTS OF NACUA'S 2018 COMPLIANCE SURVEY

June 24-27, 2018

Craig A. Alexander
National Association of College and University Attorneys

Leyda L. Benitez
Villanova University

I. Introduction

A. In the spring of 2018 NACUA conducted its second survey of chief legal officers at NACUA member institutions to gather data on current and planned compliance programs, the structure of those programs, and their perceived effectiveness. More than 200 member institutions responded. The survey also provides useful data on the make-up of offices of the general counsel and their responsibility for compliance matters.

B. NACUA conducted an initial compliance survey in the spring of 2013. The 2018 survey followed the same format as the initial 2013 survey so the results would be comparable. The 2018 survey results were compiled in an 87-page report distributed to respondents earlier this month. The full report on the 2018 compliance survey is available here. The report on the 2013 compliance survey is available here.

C. This summary highlights the key findings of the 2018 summary and compares those with the findings from the 2013 survey. One caveat: the universe of respondents in the two surveys was not the same; this should be considered when reviewing the results of the two surveys.

II. Responding Institutions

A. NACUA invited Chief Legal Officers of 606 member institutions to participate in the 2018 compliance survey and 213 completed the survey, an excellent response rate of 35%. A list of the institutions who responded is on pages 5 and 6 of the survey report. The 2013 survey was completed by 210 institutions.

B. As was the case with the 2013 survey, the 2018 survey provides data on a disaggregated basis for several discrete subgroups of respondents:

1. Type of entity (single-unit, institution within a multi-campus system, and central office of a system).
2. Public institutions and private institutions.
3. Carnegie classification.
4. Size of institutional annual operating budget (ranging in size from less than $100 million to $1 billion or more).

5. The number of full-time-equivalent students enrolled at the institution (from fewer than 5,000 to more than 35,000).

Reporting in this disaggregated way facilitates comparisons by individual institutions with institutions that have similar characteristics.

C. The make-up of responding institutions in the two surveys across these characteristics are remarkably similar and they represent an excellent cross section of NACUA institutions, as the table below indicates:

Characteristic	***Percentage of Respondents***	
	2018	***2013***
Single unit institution	70.0%	67.0%
Institution within a system	19.5%	19.4%
System Office	10.5%	13.6%
Public	51.7%	50.2%
Private	48.3%	49.8%
Doctorate-granting universities	60.2%	56.0%
Master's colleges and universities	19.4%	26.8%
Baccalaureate colleges	9.5%	11.0%
Associate's colleges	8.5%	5.7%
Special focus institutions	1.9%	0.5%
Tribal colleges	0.5%	0.0%
Annual budget less than $100 million	18.7%	16.5%
Annual budget $100-200 million	20.6%	23.5%
Annual budget $200-500 million	24.4%	22.5%
Annual budget $500 million to $1 billion	12.0%	15.0%
Annual budget $1 billion or more	24.5%	22.5%
Enrollment of fewer than 5,000 students	27.4%	26.3%
Enrollment of 5,000 to 9,999 students	17.9%	20.3%
Enrollment of 10,000 to 15,999 students	16.9%	14.7%
Enrollment of 16,000 to 24,999 students	15.9%	14.2%
Enrollment of 25,000 to 34,999 students	8.5%	10.2%
Enrollment of 35,000 or more students	13.4%	14.3%

III. Staffing in the Office of the General Counsel; Responsibility for Compliance

A. In addition to providing information about institutional compliance programs, the survey also yields interesting information about the composition of offices of general counsel. **In general, there has been an increase in the number of attorneys and of full-time equivalent employees in the office of the general counsel at member institutions over the past five years. Of those institutions reporting an increase in the number of employees in the office of the general counsel, 76.2% said the increase is attributable in whole or in part to additional compliance responsibilities at the institution.** In the 2013 survey, 70.4% of institutions that reported an increase in OGC employees said the increase was attributable in whole or in part to additional compliance responsibilities.

B. The reported average number of attorneys in the office of the general counsel increased by 1.1 since the time of the 2013 survey (from 4.1 to 5.2). The average, of course, varies by type and size of institution. In general, offices of the general counsel in system offices and at institutions with higher budgets and enrollments showed the most increase in the number of attorneys since 2013.

Characteristic	***Average number of full-time equivalent attorneys in the office of the general counsel***	
	2018	***2013***
All Institutions	5.2	4.1
Single unit institution	4.1	3.3
Institution within a system	5.2	5.0
System Office	13.6	7.5
Doctorate-granting universities	7.2	6.0
Master's colleges and universities	2.4	2.2
Baccalaureate colleges	1.6	1.3
Associate's colleges	2.0	1.4
Annual budget less than $100 million	1.7	1.1
Annual budget $100-200 million	1.6	1.6
Annual budget $200-500 million	2.9	2.7
Annual budget $500 million to $1 billion	3.9	4.7
Annual budget $1 billion or more	14.1	10.2
Enrollment of fewer than 5,000 students	1.6	1.5
Enrollment of 5,000 to 9,999 students	2.1	2.6
Enrollment of 10,000 to 15,999 students	4.8	4.9
Enrollment of 16,000 to 24,999 students	5.1	4.2
Enrollment of 25,000 to 34,999 students	9.4	5.1
Enrollment of 35,000 or more students	14.9	9.5

C. Just under half of the respondents said the number of full-time equivalent employees in their office of the general counsel increased during the past five years; the average increase for those offices was two employees.

D. **Offices of general counsel at institutions of higher education are all involved in institutional compliance efforts, some more directly than others**:

1. 99.3% of all Chief Legal Officers in both surveys responded that they provide support for their institution's compliance program.

2. Just over 31% (in both 2018 and 2013) of Chief Legal Officers indicated they have responsibility for or oversight of a formal compliance program at their institution.

3. For those institutions without a Chief Compliance Officer, 34.4% of respondents indicate that the general counsel has primary responsibility for compliance, up from 25% in 2013. Among institutions with a budget of less than $100 million annually having no Chief Compliance Officer, 54.8% report that the general counsel has primary responsibility for the institution's compliance program.

4. Those indicating that an attorney in the office of general counsel is assigned formal responsibilities for compliance increased from 29.1% of respondents in 2013 to 36.5% of respondents in 2018.

5. Nearly 98% of Chief Legal Officers rated compliance as "the most challenging issue" (4.4%) their offices face, "among the top three most challenging issues" (67.6%), or "just as challenging as any other legal issue" (25.6%). This is essentially unchanged since 2013.

IV. Institutional Compliance Function at Institutions of Higher Education

A. Overall, as might be expected, it appears that **compliance functions generally are more widely and formally adopted at institutions of higher education than they were five years ago.** Selected statistics that support this finding are:

1. The proportion of institutions reporting that they have a Chief Compliance Officer increased substantially to 34.1% in 2018 compared to only 19.5% in 2013. This varies significantly by the size of institution. In the 2018 survey, among the largest institutions (by annual budget), 62.8% of the institutions reported that they have a Chief Compliance Officer while only 15.4% of the smallest institutions have a Chief Compliance Officer.

2. For institutions with a designated Chief Compliance Officer, the percentage who are attorneys increased slightly to 27.7% in 2018 from 24.6% in 2013.

3. For those institutions without a Chief Compliance Officer, the percentage of institutions indicating that no one has primary responsibility for compliance decreased to 18.4% in 2018 from 22.2% in 2013.

4. Institutions indicating they have a formal compliance program in place increased to 47.2% from 31.2% in 2013.

5. Institutions with no formal function in place, planned, or in development dropped from 29.7% in 2013 to 25.7% in the current study.

6. The table following on the next page depicts whether responding institutions have a compliance office or offices in place, or are planning or developing a compliance office or offices. By nearly every subcategory, a greater proportion of institutions have a compliance program in place, in planning, or under development now than did so in 2013.

Characteristic	*Percentage of Respondents That*			
	2018			*2013*
	Have a compliance office or offices	*Are planning or developing a compliance office*	*Total*	*Total*
All institutions	47.2%	27.1%	74.3%	70.3%
Single unit institution	43.5%	29.6%	73.1%	68.5%
Institution within a system	62.5%	15.0%	77.5%	78.3%
System Office	50.0%	27.2%	77.2%	69.2%
Public	48.1%	25.9%	74.0%	71.6%
Private	46.0%	29.0%	75.0%	68.6%
Doctorate-granting universities	60.8%	22.4%	83.2%	82.2%
Master's colleges and universities	24.4%	34.1%	58.5%	54.7%
Baccalaureate colleges	25.0%	30.0%	55.0%	57.2%
Associate's colleges	29.5%	35.3%	64.8%	54.6%
Annual budget less than $100 million	30.8%	30.8%	61.6%	54.9%
Annual budget $100-200 million	14.2%	45.3%	59.5%	54.3%
Annual budget $200-500 million	59.9%	23.5%	83.4%	74.5%
Annual budget $500 million to $1 billion	44.0%	28.0%	72.0%	75.0%
Annual budget $1 billion or more	76.5%	13.8%	90.2%	88.4%
Enrollment of fewer than 5,000 students	29.1%	34.6%	63.6%	55.1%
Enrollment of 5,000 to 9,999 students	38.9%	27.8%	66.7%	70.0%
Enrollment of 10,000 to 15,999 students	50.0%	29.4%	79.4%	75.9%
Enrollment of 16,000 to 24,999 students	50.0%	25.0%	75.0%	84.6%
Enrollment of 25,000 to 34,999 students	82.4%	5.9%	88.3%	73.7%
Enrollment of 35,000 or more students	59.2%	25.9%	85.1%	74.1%

B. **As was the case in 2013, at institutions having a compliance office or offices, there is a wide divergence in approaches to organization and reporting lines.** There is no one compliance approach that is a consensus approach among reporting institutions.

1. A significant and growing proportion of institutions report that their Chief Compliance Officer reports directly to the CEO or President, with 12.3% indicating this in 2018 compared with 5.6% in 2013. Other reporting relationships for the Chief Compliance Officer in the 2018 survey included reporting to the General Counsel (14.4%), the Chief Financial Officer (8.9%), the Chief Internal Auditor (4.8%), the Chief Operating Officer (2.1%), the Chief Academic Officer (2.1%), and the Chief Risk Officer (0.7%).

2. There was a shift in the compliance structure reported by respondents in this survey compared with the 2013 responses. In 2013, a larger proportion of respondents (35.4%) reported that their compliance structure was decentralized without designated compliance officers compared with 24.8% of respondents reporting that structure in 2018. In the current survey, those with some centralization of their compliance function increased to 36.9% from 27.2% five years ago. The percentage of institutions reporting no formal compliance structure or function increased to 6.3% from 1.5% five years ago.

V. Areas of Greatest Compliance Risk

A. The survey, as it did in 2013, asked respondents to rank their top five areas of highest risk relative to college and university compliance.

1. Human Resources was the top area of highest risk in 2013 but in 2018 it was ranked a distant third behind Title IX and Information Security. Those two areas jumped considerably relative to the 2013 survey. In 2013, only 5.8% (each) of respondents chose Title IX and Information Security as the top area of compliance risk compared with 26.6% and 17.2%, respectively, this year.

2. In 2013, the top three areas of highest risk were Human Resources (15.2%), Financial Aid (9.4%), and Athletics (6.3%). As noted, Title IX and Information Security were tied for fourth highest at 5.8% each.

3. In 2018, the top three areas of highest risk are Title IX (26.6%), Information Security (17.2%), and Human Resources (7.4%). Financial Aid (5.9%) is fourth and Athletics (4.4%) is fifth.

B. A list of the top ten areas of highest compliance risk in the 2018 survey follows.

2018 Survey ***Top Ten Areas of Highest Risk Relative to College and University Compliance***		
Rank	***Identified Area of Highest Risk***	***% of Respondents***
1	Title IX	26.6%
2	Information Security	17.2%
3	Human Resources	7.4%
4	Financial Aid	5.9%
5	Athletics (including NCAA)	4.4%
6	Accreditation	3.9%
6	Americans with Disabilities Act (ADA)	3.9%
6	Environmental Health and Safety	3.9%
9	Sexual Harassment	3.0%
10	Governance	2.5%
10	Public Safety/Clery Act/Crime & Fire Reporting	2.5%
10	Research (animal or human subjects)	2.5%

VI. Benefits of an Effective Institutional Compliance Program

A. More than half of respondents in the 2018 compliance survey find that their institutional compliance programs are effective or very effective in sharpening the focus of internal audits and improving the ability to work with external auditors and risk management consultants (59.6%), reducing negative experiences with external compliance audits and inspections (55.3%), and making supervisors more aware of the importance of compliance in evaluating employee performance (50.3%).

B. Fewer respondents, but still a significant proportion, find that their institutional compliance programs are effective or very effective in substantially reducing complaints in internal university proceedings and in external courts and government agencies (47.2%) and improving insurance claims and substantially reducing insurance premiums (37.6%).

C. Overall, the respondents in this year's survey ranked the benefits of an effective compliance program about the same as the rankings in the 2013 survey, as shown in the following summary table (data show the proportion of those reporting the item as effective or very effective):

Benefit of an Effective Compliance Program:	***2018***	***2013***
Sharpens focus of internal audits and improves ability to work with external auditors and risk management consultants	59.6%	58.6%
Reduced negative experiences with external compliance audits and inspections	55.3%	56.9%
Supervisors are more aware of the importance of compliance in evaluating employee performance	50.3%	52.0%
Substantially reduced complaints in internal university proceedings and in external courts and government agencies	47.2%	45.8%
Improved insurance claims experience and substantially reduced insurance premiums	37.6%	36.1%

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

Guidance Document
Updated: April 2019

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated April 2019)

Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, the memorandum entitled "Selection of Monitors in Criminal Division Matters" issued by Assistant Attorney General Brian Benczkowski (hereafter, the "Benczkowski Memo") instructs prosecutors to consider, at the time of the resolution, "whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems" and "whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future" to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make an individualized determination in each case. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated April 2019)

1. "Is the corporation's compliance program well designed?"
2. "Is the program being applied earnestly and in good faith?" In other words, is the program being implemented effectively?
3. "Does the corporation's compliance program work" in practice?

See JM § 9-28.800.

In answering each of these three "fundamental questions," prosecutors may evaluate the company's performance on various topics that the Criminal Division has frequently found relevant in evaluating a corporate compliance program. The sample topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue.[1] Even though we have organized the topics under these three fundamental questions, we recognize that some topics necessarily fall under more than one category.

I. Is the Corporation's Compliance Program Well Designed?

The "critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct." JM 9-28.800.

Accordingly, prosecutors should examine "the comprehensiveness of the compliance program," JM 9-28.800, ensuring that there is not only a clear message that misconduct is not tolerated, but also policies and procedures – from appropriate assignments of responsibility, to training programs, to systems of incentives and discipline – that ensure the compliance program is well-integrated into the company's operations and workforce.

A. Risk Assessment

The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks.

Prosecutors should consider whether the program is appropriately "designed to detect the particular types of misconduct most likely to occur in a particular corporation's line of business" and "complex regulatory environment[]." JM 9-28.800.[2] For example, prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness

of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.

Prosecutors should also consider "[t]he effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment" and whether its criteria are "periodically updated." *See, e.g.*, JM 9-47-120(2)(c); U.S.S.G. § 8B2.1(c) ("the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of the compliance program] to reduce the risk of criminal conduct").

Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction in a low-risk area. Prosecutors should therefore consider, as an indicator of risk-tailoring, "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800.

- **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faces? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company's compliance program?

- **Risk-Tailored Resource Allocation –** Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors? Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?

- **Updates and Revisions** – Is the risk assessment current and subject to periodic review? Have there been any updates to policies and procedures in light of lessons learned? Do these updates account for risks discovered through misconduct or other problems with the compliance program?

B. Policies and Procedures

Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process. As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the

company's commitment to full compliance with relevant Federal laws that is accessible and applicable to all company employees. As a corollary, prosecutors should also assess whether the company has established policies and procedures that incorporate the culture of compliance into its day-to-day operations.

- **Design** – What is the company's process for designing and implementing new policies and procedures, and has that process changed over time? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?

- **Comprehensiveness** – What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?

- **Accessibility** – How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access?

- **Responsibility for Operational Integration** – Who has been responsible for integrating policies and procedures? Have they been rolled out in a way that ensures employees' understanding of the policies? In what specific ways are compliance policies and procedures reinforced through the company's internal control systems?

- **Gatekeepers** – What, if any, guidance and training has been provided to key gatekeepers in the control processes (*e.g.*, those with approval authority or certification responsibilities)? Do they know what misconduct to look for? Do they know when and how to escalate concerns?

C. Training and Communications

Another hallmark of a well-designed compliance program is appropriately tailored training and communications.

Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Prosecutors should also assess whether the company has relayed information in a manner tailored to the audience's size, sophistication, or subject matter expertise. Some companies, for instance, give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise.

Prosecutors should also assess whether the training adequately covers prior compliance incidents and how the company measures the effectiveness of its training curriculum.

Prosecutors, in short, should examine whether the compliance program is being disseminated to, and understood by, employees in practice in order to decide whether the compliance program is "truly effective." JM 9-28.800.

- **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred? Have supervisory employees received different or supplementary training? What analysis has the company undertaken to determine who should be trained and on what subjects?

- **Form/Content/Effectiveness of Training** – Has the training been offered in the form and language appropriate for the audience? Is the training provided online or in-person (or both), and what is the company's rationale for its choice? Has the training addressed lessons learned from prior compliance incidents? How has the company measured the effectiveness of the training? Have employees been tested on what they have learned? How has the company addressed employees who fail all or a portion of the testing?

- **Communications about Misconduct** – What has senior management done to let employees know the company's position concerning misconduct? What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company's policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of misconduct that leads to discipline)?

- **Availability of Guidance** – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

D. Confidential Reporting Structure and Investigation Process

Another hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual misconduct. Prosecutors should assess whether the company's complaint-handling process includes pro-active measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling

investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.

Confidential reporting mechanisms are highly probative of whether a company has "established corporate governance mechanisms that can effectively detect and prevent misconduct." JM 9-28.800; *see also* U.S.S.G. § 8B2.1(b)(5)(C) (an effectively working compliance program will have in place, and have publicized, "a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation").

- **Effectiveness of the Reporting Mechanism** – Does the company have an anonymous reporting mechanism, and, if not, why not? How is the reporting mechanism publicized to the company's employees? Has it been used? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?

- **Properly Scoped Investigations by Qualified Personnel** – How does the company determine which complaints or red flags merit further investigation? How does the company ensure that investigations are properly scoped? What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented? How does the company determine who should conduct an investigation, and who makes that determination?

- **Investigation Response** – Does the company apply timing metrics to ensure responsiveness? Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?

- **Resources and Tracking of Results** – Are the reporting and investigating mechanisms sufficiently funded? How has the company collected, tracked, analyzed, and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses?

E. Third Party Management

A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the degree of appropriate due diligence may vary based on the size

and nature of the company or transaction, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions.

Prosecutors should also assess whether the company knows its third-party partners' reputations and relationships, if any, with foreign officials, and the business rationale for needing the third party in the transaction. For example, a prosecutor should analyze whether the company has ensured that contract terms with third parties specifically describe the services to be performed, that the third party is actually performing the work, and that its compensation is commensurate with the work being provided in that industry and geographical region. Prosecutors should further assess whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.

In sum, a company's third-party due diligence practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect the particular types of misconduct most likely to occur in a particular corporation's line of business." JM 9-28.800.

- **Risk-Based and Integrated Processes** – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

- **Appropriate Controls** – How does the company ensure there is an appropriate business rationale for the use of third parties? If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties? What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

- **Management of Relationships** – How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its third party relationship

managers about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties?

- **Real Actions and Consequences** – Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date? If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues?

F. Mergers and Acquisitions (M&A)

A well-designed compliance program should include comprehensive due diligence of any acquisition targets. Pre-M&A due diligence enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete due diligence can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability.

The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization.

- **Due Diligence Process** – Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?

- **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?

- **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures at new entities?

II. Is the Corporation's Compliance Program Being Implemented Effectively?

Even a well-designed compliance program may be unsuccessful in practice if implementation is lax or ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a "paper program" or one "implemented, reviewed, and revised, as appropriate, in an effective manner." JM 9-28.800. In addition, prosecutors should determine "whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts." JM 9-28.800. Prosecutors should also determine "whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's commitment to it." JM 9-28.800; *see also* JM 9-47.120(2)(c) (criteria for an effective compliance program include "[t]he company's culture of compliance, including awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated").

A. Commitment by Senior and Middle Management

Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law. The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the top.

The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them. *See* U.S.S.G. § 8B2.1(b)(2)(A)-(C) (the company's "*governing authority* shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight" of it; "[*h*]*igh-level personnel* … shall ensure that the organization has an effective compliance and ethics program" (emphasis added)).

- **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How have they modelled proper behavior to subordinates? Have managers tolerated greater compliance risks in pursuit of new business or greater revenues? Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?

- **Shared Commitment** – What actions have senior leaders and middle-management stakeholders (*e.g.*, business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts? Have they persisted in that commitment in the face of competing interests or business objectives?

- **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

B. Autonomy and Resources

Effective implementation also requires those charged with a compliance program's day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured. Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee. The sufficiency of each factor, however, will depend on the size, structure, and risk profile of the particular company. "A large organization generally shall devote more formal operations and greater resources . . . than shall a small organization." Commentary to U.S.S.G. § 8B2.1 note 2(C). By contrast, "a small organization may [rely on] less formality and fewer resources." *Id.* Regardless, if a compliance program is to be truly effective, compliance personnel must be empowered within the company.

Prosecutors should evaluate whether "internal audit functions [are] conducted at a level sufficient to ensure their independence and accuracy," as an indicator of whether compliance personnel are in fact empowered and positioned to "effectively detect and prevent misconduct." JM 9-28.800. Prosecutors should also evaluate "[t]he resources the company has dedicated to compliance," "[t]he quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk," and "[t]he authority and independence of the compliance function and the availability of compliance expertise to the board." JM 9-47.120(2)(c); *see also* JM 9-28.800 (instructing prosecutors to evaluate whether "the directors established an information and reporting system in the organization reasonably designed to provide management and directors with timely and accurate information sufficient to allow them to reach an informed decision regarding the organization's compliance with the law"); U.S.S.G. § 8B2.1(b)(2)(C) (those with "day-to-day operational

responsibility" shall have "adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority").

- **Structure** – Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report? Is the compliance function run by a designated chief compliance officer, or another executive within the company, and does that person have other roles within the company? Are compliance personnel dedicated to compliance responsibilities, or do they have other, non-compliance responsibilities within the company? Why has the company chosen the compliance structure it has in place?

- **Seniority and Stature** – How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company's strategic and operational decisions? How has the company responded to specific instances where compliance raised concerns? Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?

- **Experience and Qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? Who reviews the performance of the compliance function and what is the review process?

- **Funding and Resources** – Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same? Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?

- **Autonomy** – Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of the senior management present for these meetings? How does the company ensure the independence of the compliance and control personnel?

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? What level of access does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

C. Incentives and Disciplinary Measures

Another hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance. Prosecutors should assess whether the company has clear disciplinary procedures in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) ("the organization's compliance program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct").

By way of example, some companies have found that publicizing disciplinary actions internally, where appropriate, can have valuable deterrent effects. At the same time, some companies have also found that providing positive incentives – personnel promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership – have driven compliance. Some companies have even made compliance a significant metric for management bonuses and/or have made working on compliance a means of career advancement.

- **Human Resources Process** – Who participates in making disciplinary decisions, including for the type of misconduct at issue? Is the same process followed for each instance of misconduct, and if not, why? Are the actual reasons for discipline communicated to employees? If not, why not? Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?

- **Consistent Application** – Have disciplinary actions and incentives been fairly and consistently applied across the organization? Are there similar instances of misconduct that were treated disparately, and if so, why?

- **Incentive System** – Has the company considered the implications of its incentives and rewards on compliance? How does the company incentivize compliance and ethical behavior? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied) as a result of compliance and ethics considerations? Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel?

III. Does the Corporation's Compliance Program Work in Practice?

The Principles of Federal Prosecution of Business Organizations require prosecutors to assess "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision." JM 9-28.300. Due to the backward-looking nature of the first inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.

In answering this question, it is important to note that the existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense. *See* U.S.S.G. § 8B2.1(a) ("[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct"). Indeed, "[t]he Department recognizes that no compliance program can ever prevent all criminal activity by a corporation's employees." JM 9-28.800. Of course, if a compliance program did effectively identify misconduct, including allowing for timely remediation and self-reporting, a prosecutor should view the occurrence as a strong indicator that the compliance program was working effectively.

In assessing whether a company's compliance program was effective at the time of the misconduct, prosecutors should consider whether and how the misconduct was detected, what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company's remedial efforts.

To determine whether a company's compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future.

For example, prosecutors should consider, among other factors, "whether the corporation has made significant investments in, and improvements to, its corporate compliance

program and internal controls systems" and "whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future." Benczkowski Memo at 2 (observing that "[w]here a corporation's compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will not likely be necessary").

A. Continuous Improvement, Periodic Testing, and Review

One hallmark of an effective compliance program is its capacity to improve and evolve. The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company's size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47-120(2)(c) (looking to "[t]he auditing of the compliance program to assure its effectiveness"). Prosecutors should likewise look to whether a company has taken "reasonable steps" to "ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct," and "evaluate periodically the effectiveness of the organization's" program. U.S.S.G. § 8B2.1(b)(5). Proactive efforts like these may not only be rewarded in connection with the form of any resolution or prosecution (such as through remediation credit or a lower applicable fine range under the Sentencing Guidelines), but more importantly, may avert problems down the line.

- **Internal Audit** – What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? How are audits carried out? What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often does internal audit conduct assessments in high-risk areas?

- **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third-parties does the company undertake? How are the results reported and action items tracked?

- **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?

- **Culture of Compliance** – How often and how does the company measure its culture of compliance? Does the company seek input from all levels of employees to determine whether they perceive senior and middle management's commitment to compliance? What steps has the company taken in response to its measurement of the compliance culture?

B. Investigation of Misconduct

Another hallmark of a compliance program that is working effectively is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company's response, including any disciplinary or remediation measures taken.

- **Properly Scoped Investigation by Qualified Personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

- **Response to Investigations** – Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory manager and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

C. Analysis and Remediation of Any Underlying Misconduct

Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on "the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47.120(3)(c) ("to receive full credit for timely and appropriate remediation" under the FCPA Corporate Enforcement Policy, a company should demonstrate "a root cause analysis" and, where appropriate, "remediation to address the root causes").

Prosecutors should consider "any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program." JM 98-28.800; *see also* JM 9-47-120(2)(c) (looking to "[a]ppropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred" and "any additional steps that demonstrate recognition of the seriousness of the misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risk").

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?

- **Prior Weaknesses** – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

- **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

- **Vendor Management** – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company's analysis of why such opportunities were missed?

- **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

- **Accountability** – What disciplinary actions did the company take in response to the misconduct and were they timely? Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision? What is the company's record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue?

---

[1] Many of the topics also appear in the following resources:

- Justice Manual ("JM")
  - JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual ("JM"), *available at* https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.
  - JM 9-47.120 FCPA Corporate Enforcement Policy, *available at* https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.
- Chapter 8 – Sentencing of Organizations - United States Sentencing Guidelines ("U.S.S.G."), *available at* https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8#NaN.

- Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Brian Benczkowski on October 11, 2018, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download.
- Criminal Division corporate resolution agreements, *available at* https://www.justice.gov/news (DOJ's Public Affairs website contains press releases for all Criminal Division corporate resolutions which contain links to charging documents and agreements).
- A Resource Guide to the U.S. Foreign Corrupt Practices Act ("FCPA Guide") published in November 2012 by the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) *available at* https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.
- Good Practice Guidance on Internal Controls, Ethics, and Compliance adopted by the Organization for Economic Co-operation and Development ("OECD") Council on February 18, 2010 *available at* https://www.oecd.org/daf/anti-bribery/44884389.pdf.
- Anti-Corruption Ethics and Compliance Handbook for Business ("OECD Handbook") published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank *available at* https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf.

[2] As discussed in the Justice Manual, many companies operate in complex regulatory environments outside the normal experience of criminal prosecutors. JM 9-28.000. For example, financial institutions such as banks, subject to the Bank Secrecy Act statute and regulations, require prosecutors to conduct specialized analyses of their compliance programs in the context of their anti-money laundering requirements. Consultation with the Money Laundering and Asset Recovery Section is recommended when reviewing AML compliance. *See* https://www.justice.gov/criminal-mlars. Prosecutors may also wish to review guidance published by relevant federal and state agencies. *See* Federal Financial Institutions Examination Council/Bank Secrecy Act/Anti-Money Laundering Examination Manual, *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm).

THE IIA'S THREE LINES MODEL

An update of the Three Lines of Defense

The Institute of Internal Auditors | Global

Table of Contents

INTRODUCTION

Organizations are human undertakings, operating in an increasingly uncertain, complex, interconnected, and volatile world. They often have multiple stakeholders with diverse, changeable, and sometimes competing interests. Stakeholders entrust organizational oversight to a governing body, which in turn delegates resources and authority to management to take appropriate actions, including managing risk.

For these reasons and more, organizations need effective structures and processes to enable the achievement of objectives, while supporting strong governance and risk management. As the governing body receives reports from management on activities, outcomes, and forecasts, both the governing body and management rely on internal audit to provide independent, objective assurance and advice on all matters and to promote and facilitate innovation and improvement. The governing body is ultimately accountable for governance, which is achieved through the actions and behaviors of the governing body as well as management and internal audit.

The Three Lines Model helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management. The model applies to all organizations and is optimized by:

Key terms

Organization – An organized group of activities, resources, and people working toward shared goals.

Stakeholders – Those groups and individuals whose interests are served or impacted by the organization.

Governing body – Those individuals who are accountable to stakeholders for the success of the organization.

Management – Those individuals, teams, and support functions assigned to provide products and/or services to the organization's clients.

Internal audit – Those individuals operating independently from management to provide assurance and insight on the adequacy and effectiveness of governance and the management of risk (including internal control).

The Three Lines Model – The model previously known as the Three Lines of Defense.

Internal control – Processes designed to provide reasonable confidence over the achievement of objectives.

- Adopting a principles-based approach and adapting the model to suit organizational objectives and circumstances.
- Focusing on the contribution risk management makes to achieving objectives and creating value, as well as to matters of "defense" and protecting value.
- Clearly understanding the roles and responsibilities represented in the model and the relationships among them.
- Implementing measures to ensure activities and objectives are aligned with the prioritized interests of stakeholders.

PRINCIPLES OF THE THREE LINES MODEL

Principle 1: Governance

Governance of an organization requires appropriate structures and processes that enable:

- **Accountability** by a governing body to stakeholders for organizational oversight through integrity, leadership, and transparency.
- **Actions** (including managing risk) by management to achieve the objectives of the organization through risk-based decision-making and application of resources.
- **Assurance and advice** by an independent internal audit function to provide clarity and confidence and to promote and facilitate continuous improvement through rigorous inquiry and insightful communication.

Key terms

Risk-based decision-making – A considered process that includes analysis, planning, action, monitoring, and review, and takes account of potential impacts of uncertainty on objectives.

Assurance – Independent confirmation and confidence.

Principle 2: Governing body roles

The governing body ensures:

- Appropriate structures and processes are in place for effective governance.
- Organizational objectives and activities are aligned with the prioritized interests of stakeholders.

The governing body:

- Delegates responsibility and provides resources to management to achieve the objectives of the organization while ensuring legal, regulatory, and ethical expectations are met.
- Establishes and oversees an independent, objective, and competent internal audit function to provide clarity and confidence on progress toward the achievement of objectives.

Principle 3: Management and first and second line roles

Management's responsibility to achieve organizational objectives comprises both first and second line roles.[1] *First line roles* are most directly aligned with the delivery of products and/or services to clients of the organization, and include the roles of support functions[2]. *Second line roles* provide assistance with managing risk.

First and second line roles may be blended or separated. Some second line roles may be assigned to specialists to provide complementary expertise, support, monitoring, and challenge to those with first line roles. Second line roles can focus on specific objectives of risk management, such as: compliance with laws, regulations, and acceptable ethical behavior; internal control; information and technology security; sustainability; and quality assurance. Alternatively, second line roles may span a broader responsibility for risk management, such as enterprise risk management (ERM). However, responsibility for managing risk remains a part of first line roles and within the scope of management.

Principle 4: Third line roles

Internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management.[3] It achieves this through the competent application of systematic and disciplined processes, expertise, and insight. It reports its findings to management and the governing body to promote and facilitate continuous improvement. In doing so, it may consider assurance from other internal and external providers.

Principle 5: Third line independence

Internal audit's independence from the responsibilities of management is critical to its objectivity, authority, and credibility. It is established through: accountability to the governing body; unfettered access to people, resources, and data needed to complete its work; and freedom from bias or interference in the planning and delivery of audit services.

Principle 6: Creating and protecting value

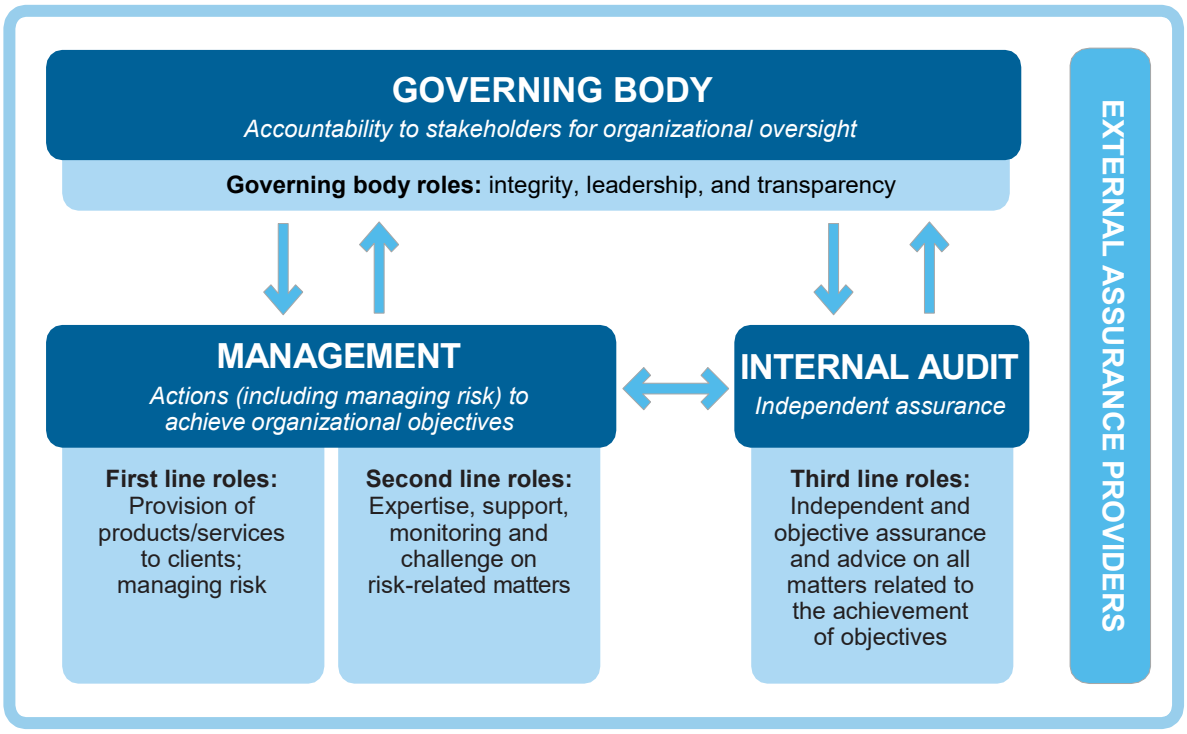
All roles working together collectively contribute to the creation and protection of value when they are aligned with each other and with the prioritized interests of stakeholders. Alignment of activities is achieved through communication, cooperation, and collaboration. This ensures the reliability, coherence, and transparency of information needed for risk-based decision making.

1. The language of "first line," "second line," and "third line" is retained from the original model in the interests of familiarity. However, the "lines" are not intended to denote structural elements but a useful differentiation in roles. Logically, governing body roles also constitute a "line" but this convention has not been adopted to avoid confusion. The numbering (first, second, third) should not be taken to imply sequential operations. Instead, all roles operate concurrently.

2. Some consider the roles of support functions (such as HR, administration, and building services) to be second line roles. For clarity, the Three Lines Model regards *first line roles* to include both "front of house" and "back office" activities, and *second line roles* to comprise those complementary activities focused on risk-related matters.

3. In some organizations, other third line roles are identified, such as oversight, inspection, investigation, evaluation, and remediation, which may be part of the internal audit function or operate separately.

The IIA's Three Lines Model



KEY ROLES IN THE THREE LINES MODEL

Organizations differ considerably in their distribution of responsibilities. However, the following high-level roles serve to amplify the Principles of the Three Lines Model.

The governing body

- Accepts accountability to stakeholders for oversight of the organization.
- Engages with stakeholders to monitor their interests and communicate transparently on the achievement of objectives.
- Nurtures a culture promoting ethical behavior and accountability.
- Establishes structures and processes for governance, including auxiliary committees as required.
- Delegates responsibility and provides resources to management for achieving the objectives of the organization.
- Determines organizational appetite for risk and exercises oversight of risk management (including internal control).
- Maintains oversight of compliance with legal, regulatory, and ethical expectations.
- Establishes and oversees an independent, objective, and competent internal audit function.

Management

First line roles

- Leads and directs actions (including managing risk) and application of resources to achieve the objectives of the organization.
- Maintains a continuous dialogue with the governing body, and reports on: planned, actual, and expected outcomes linked to the objectives of the organization; and risk.
- Establishes and maintains appropriate structures and processes for the management of operations and risk (including internal control).
- Ensures compliance with legal, regulatory, and ethical expectations.

Second line roles

- Provides complementary expertise, support, monitoring, and challenge related to the management of risk, including:
    - The development, implementation, and continuous improvement of risk management practices (including internal control) at a process, systems, and entity level.
    - The achievement of risk management objectives, such as: compliance with laws, regulations, and acceptable ethical behavior; internal control; information and technology security; sustainability; and quality assurance.
- Provides analysis and reports on the adequacy and effectiveness of risk management (including internal control).

Internal audit

- Maintains primary accountability to the governing body and independence from the responsibilities of management.
- Communicates independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management (including internal control) to support the achievement of organizational objectives and to promote and facilitate continuous improvement.
- Reports impairments to independence and objectivity to the governing body and implements safeguards as required.

External assurance providers

- Provide additional assurance to:
    - Satisfy legislative and regulatory expectations that serve to protect the interests of stakeholders.
    - Satisfy requests by management and the governing body to complement internal sources of assurance.

RELATIONSHIPS AMONG CORE ROLES

Between the governing body and management (both first and second line roles)

The governing body typically sets the direction of the organization by defining the vision, mission, values, and organizational appetite for risk. It then delegates responsibility for the achievement of the organization's objectives to management, along with the necessary resources. The governing body receives reports from management on planned, actual, and expected outcomes, as well as reports on risk and the management of risk.

Key term

Chief Executive Officer (CEO) – The most senior individual in the organization with responsibility over operations.

Organizations vary as to the degree of overlap and separation between the roles of the governing body and management. The governing body can be more or less "hands on" with respect to strategic and operational matters. Either the governing body or management may take the lead in developing the strategic plan, or it may be a shared undertaking. In some jurisdictions, the Chief Executive Officer (CEO) may be a member of the governing body and may even be its chair. In all cases, there needs to be strong communication between management and the governing body. The CEO is typically the focal point for this communication, but other senior managers may have frequent interactions with the governing body. Organizations may wish, and their regulators may require, leaders of second line roles such as a Chief Risk Officer (CRO) and a Chief Compliance Officer (CCO) to have a direct reporting line to the governing body. This is fully consistent with the Principles of the Three Lines Model.

Between management (both first and second line roles) and internal audit

Internal audit's independence from management ensures it is free from hindrance and bias in its planning and in the carrying out of its work, enjoying unfettered access to the people, resources, and information it requires. It is accountable to the governing body. However, independence does not imply isolation. There must be regular interaction between internal audit and management to ensure the work of internal audit is relevant and aligned with the strategic and operational needs of the organization. Through all of its activities, internal audit builds its knowledge and understanding of the organization, which contributes to the assurance and advice it delivers as a trusted advisor and strategic partner. There is a need for collaboration and communication across both the first and second line roles of management and internal audit to ensure there is no unnecessary duplication, overlap, or gaps.

Between internal audit and the governing body

Internal audit is accountable to, and sometimes described as being the "eyes and ears" of, the governing body.

The governing body is responsible for oversight of internal audit, which requires: ensuring an independent internal audit function is established, including the hiring and firing of the Chief Audit Executive (CAE); serving as the primary reporting line for the CAE[4]; approving and resourcing the audit plan; receiving and considering reports from the CAE; and enabling free access by the CAE to the governing body, including private sessions without the presence of management.

Key term

Chief Audit Executive (CAE) – **The most senior individual in the organization with responsibility for internal audit services, often known as the Head of Internal Audit or similar title.**

Among all roles

The governing body, management, and internal audit have their distinct responsibilities, but all activities need to be aligned with the objectives of the organization. The basis for successful coherence is regular and effective coordination, collaboration, and communication.

4. For administrative purposes, the CAE may also report to an appropriately senior level of management.

APPLYING THE MODEL

Structure, roles, and responsibilities

The Three Lines Model is most effective when it is adapted to align with the objectives and circumstances of the organization. How an organization is structured and how roles are assigned are matters for management and the governing body to determine. The governing body may establish committees to provide additional oversight for particular aspects of its responsibility, such as audit, risk, finance, planning, and compensation. Within management, there are likely to be functional and hierarchical arrangements and an increasing tendency toward specialization as organizations grow in size and complexity.

Functions, teams, and even individuals may have responsibilities that include both first and second line roles. However, direction and oversight of second line roles may be designed to secure a degree of independence from those with first line roles — and even from the most senior levels of management — by establishing primary accountability and reporting lines to the governing body. The Three Lines Model allows for as many reporting lines between management and the governing body as required. In some organizations, most notably regulated financial institutions, there is a statutory requirement for such arrangements to ensure sufficient independence. Even in these situations, those in management with first line roles remain responsible for managing risk.

Second line roles may include monitoring, advice, guidance, testing, analyzing, and reporting on matters related to the management of risk. Insofar as these provide support and challenge to those with first line roles and are integral to management decisions and actions, second line roles are part of management's responsibilities and are never fully independent from management, regardless of reporting lines and accountabilities.

A defining characteristic of third line roles is independence from management. The Principles of the Three Lines Model describe the importance and nature of internal audit independence, setting internal audit apart from other functions and enabling the distinctive value of its assurance and advice. Internal audit's independence is safeguarded by not making decisions or taking actions that are part of management's responsibilities (including risk management) and by declining to provide assurance on activities for which internal audit has current, or has had recent, responsibility. For example, in some organizations, the CAE is asked to assume additional decision-making responsibilities over activities utilizing similar competencies, such as aspects of statutory compliance or ERM. In such circumstances, internal audit is not independent of these activities or of their results, and therefore, when the governing body seeks independent and objective assurance and advice relating to those areas, it is necessary for its provision to be undertaken by a qualified third party.

Oversight and assurance

The governing body relies on reports from management (comprising those with first and second line roles), internal audit, and others in order to exercise oversight and achievement of its objectives, for which it is accountable to stakeholders. Management provides valuable assurance (also referred to as attestations) on planned, actual, and forecast outcomes, on risk, and on risk management by drawing upon direct experience and expertise. Those with second line roles provide additional assurance on risk-related matters. Because of internal audit's independence from management, the assurance it provides carries the highest degree of objectivity and confidence beyond that which those with first and second line roles can provide to the governing body, irrespective of reporting lines. Further assurance may also be drawn from external providers.

Coordination and alignment

Effective governance requires appropriate assignment of responsibilities as well as strong alignment of activities through cooperation, collaboration, and communication. The governing body seeks confirmation through internal audit that governance structures and processes are appropriately designed and operating as intended.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

Copyright

July 2020

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org

Audit Committee **Item F.2.**
October 8, 2020

YOUTH PROTECTION AND COMPLIANCE UPDATE

REQUESTED ACTION

Item for information and discussion only.

SUMMARY

One of the areas for which the Office of Compliance and Integrity has assumed responsibility is youth protection and compliance. On September 1, Prenicia Clifton joined UW System as the Director of Youth Protection and Compliance. She will work with UW System Precollege Liaisons, program directors, and youth program coordinators to support the implementation of training, safe oversight of minors, policies, and standards for youth protection and compliance. Prenicia previously served as UW-Madison's Director of the Office of Youth Protection and Compliance.

To support youth protection and compliance efforts, Prenicia will oversee the development of a system-wide database application to maintain and track youth program compliance. For example, each program or activity that involves minors will be required to confirm the existence of youth safety plans and must upload staff rosters to ensure that all staff working with minors have received appropriate background checks. The effort will build on the functionality of an existing UW-Madison youth protection database to include the other UW System institutions. Processes for maintaining compliance and populating the database will be established for each institution, and the database will be populated with participant data for each program. This initiative will also help bolster our marketing and recruitment efforts with K-12 school districts and other youth programs around the state to build the next generation of UW System students.

Presenter(s)

- Katie Ignatowski, Chief Compliance Officer, UW System Office of Compliance and Integrity
- Prenicia Clifton, Director of Youth Protection and Compliance, UW System Office of Compliance and Integrity