### Executive Session to discuss:
- C.G.S. 1-200(6)[E] – Preliminary drafts or notes that the public agency has determined that the public’s interest in withholding such documents clearly outweighs the public interest in disclosure. [1-210(b)(1)]
- C.G.S. 1-200(6)[E] – Records or the information contained therein pertaining to strategy and negotiations with respect to pending claims [1-210(b)(4)]
- C.G.S 1-200(6)(E) – Records, reports and statements privileged by the attorney-client relationship. [1-210(b)(10)]
- C.G.S. 1-200(6)[C] – Records of standards, procedures, processes, software and codes not otherwise available to the public, the disclosure of which would compromise the security and integrity of an information technology system. [1-210(b)(20)]

### Opportunity for Public Comments
None

### Minutes of the March 7, 2019 JACC Meeting
Approval 1

### External Engagements
- Status of External Engagements
- Vizient Request to Hire
- 340B Drug Pricing Program Review

### Auditor of Public Accounts

### Storrs & UConn Health Significant Compliance Activities
- Research Compliance

### UConn Health – HealthONE Update

### Storrs & UConn Health Significant Audit Activities
- Status of Audit Assignments
- Follow Up Activities
- Audit Updates

### Informational/Educational Items
- Compliance Chatters – UConn
- Article – Healthcare Business Continuity Management and Disaster Recovery
- Article – Department of Justice, Evaluation of Corporate Compliance Programs

### Conclusion of Full Meeting

### Information Session with OACE and External Auditors

The next meeting of the JACC will be held on Thursday, September 19, 2019 at 10:00 am
University of Connecticut, Wilbur Cross, North Reading Room, Mansfield Way, Storrs, CT
University of Connecticut & University of Connecticut Health Center

Joint Audit & Compliance Committee Meeting
The meeting of the Joint Audit and Compliance Committee (JACC) was called to order at 10:15 a.m. by Trustee Nayden.

**ON A MOTION** made by Trustee Gouin and seconded by Trustee Carbray, the JACC voted to go into executive session to discuss:

- C.G.S. 1-200(6)[E] – Preliminary drafts or notes that the public agency has determined that the public’s interest in withholding such documents clearly outweighs the public interest in disclosure. [1-210(b)(1)]
- C.G.S. 1-200(6)[E] – Records or the information contained therein pertaining to strategy and negotiations with respect to pending claims
- C.G.S. 1-200(6)[E] – Records, reports and statements privileged by the attorney-client relationship. [1-210(b)(10)]
- C.G.S. 1-200(6)[C] – Records of standards, procedures, processes, software, and codes not otherwise available to the public, the disclosure of which would compromise the security and integrity of an information technology system. [1-210(b)(20)]

Executive Session was attended by the following: **Joint Audit & Compliance Committee members:** R. Carbray, J. Freedman, J. Gouin, T. Holt, and D. Nayden; **Audit Staff members:** C. Chiaputti, H. Hildebrandt, A. Marsh, G. Perrotti, A. Quaresima, and E. Zincavage; **Compliance Staff members:** K. Fearney, K. Hill, and E. Vitullo; **Senior Staff:** C. Andrews, W. Byerly, J. Elliott, R. Rubin, J. Shoulson, and; **General Counsel:** J. Blumenthal, N. Gelston; **Portions of Executive Session were also attended by:** C. Gray, B. Metz, M. Mundrane, and R. Rudnick.

The Executive Session ended at 11:04 a.m. and the JACC returned to open session at 11:05 a.m.

There were no public comments.

**Tab 1 – Minutes of the Meeting**

**ON A MOTION** made by Trustee Nayden and seconded by Director Freedman the minutes of the December 18, 2018 JACC meeting were approved.

**Tab 2 – External Engagements**

**ON A MOTION** made by Trustee Nayden and seconded by Director Holt, the JACC approved the $50,443 fee increase proposed by Marcum, LLP for the audit of UConn Health’s John Dempsey Hospital, University Medical Group, and Finance Corporation, for the 2018 fiscal year.

**ON A MOTION** made by Trustee Nayden and seconded by Trustee Carbray, the JACC approved the $12,500 fee increase proposed by CohnReznick, LLP for the UConn 2000 expenditures audit and agreed upon procedures engagement for the 2018 fiscal year.

P. Ballasy and C. Kurth from CohnReznick presented:

- UConn 2000 Construction Projects Funded with University of Connecticut General Obligation Bonds Audit and AUP FY2018
University of Connecticut & University of Connecticut Health Center
Joint Audit & Compliance Committee Meeting

Meeting Minutes from March 7, 2019

University of Connecticut, Wilbur Cross, North Reading Room, Mansfield Way, Storrs, CT


Tab 3 – Auditor of Public Accounts
State Auditors W. Felgate, A. Phung, M. Delaney, and T. Lepore presented:
- UConn Financial Reports for the Year Ended June 30, 2018;

Tab 4 – Significant Compliance Activities
K. Fearney provided an update on compliance activities and introduced the new Associate Compliance Officer for UConn Health, Kimberly Hill.

D. Abromaitis provided an update on Healthcare and Regulatory Compliance activities at UConn Health.

Tab 5 – UConn Health – HealthONE Update
B. Metz provided the committee with a HealthONE update.

Tab 6 – Storrs & UConn Health Significant Audit Activities
C. Chiaputti provided the JACC with an update on the status of audit assignments (UConn and UConn Health). The JACC reviewed and accepted six audits. In addition, Audit and Management Advisory Services had sixteen audits in progress during this reporting period.

A. Swinney and A. Fiorvanti provided an update on NCAA Division Football Bowl Subdivision home football game attendance requirements.

Tab 7 – Informational / Educational Items
- Compliance Chatter Update;
- UConn Health Compliance Matters Newsletter.

There being no further business, ON A MOTION made by Trustee Nayden and seconded by Director Holt, the meeting was adjourned at 11:51 a.m.

Respectfully submitted,

Angela Marsh
University of Connecticut & University of Connecticut Health Center

Joint Audit & Compliance Committee Meeting
<table>
<thead>
<tr>
<th>Vendor</th>
<th>Area</th>
<th>Scope</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marcum, LLP</td>
<td>UConn Health</td>
<td>Audits of the John Dempsey Hospital and Dental Clinics (Clinical Programs Fund), including the OHCA filings, UConn Medical Group (UMG) and the University of Connecticut Health Center Finance Corporation for FY2017, 2018 and 2019.</td>
<td>The FY2019 engagement is underway.</td>
</tr>
<tr>
<td>BKD</td>
<td>UConn Athletics</td>
<td>NCAA agreed upon procedures performed on all revenues, expenses, and capital expenditures for or on behalf of the University’s Athletics Program for FY2016, 2017 and 2018. Exercising the option to extend the engagement to include FY2019 and 2020, as allowed by contract.</td>
<td>FY2019 engagement is anticipated to begin in September 2019.</td>
</tr>
<tr>
<td>CohnReznick, LLP</td>
<td>UConn &amp; UConn Health</td>
<td>Annual audit of UCONN 2000 named projects substantially completed and deferred maintenance projects with designated budgets substantially completed and annual agreed upon procedures performed on total UCONN 2000 expenditures (named projects, deferred maintenance and equipment) for FY2016, 2017 and 2018. Exercising the option to extend the engagement to include FY2019 and 2020, as allowed by contract.</td>
<td>FY2019 engagement is anticipated to begin in September 2019.</td>
</tr>
<tr>
<td>Vizient, Inc.</td>
<td>UConn Health</td>
<td>Audit of UConn Health’s John Dempsey Hospital (JDH) 340B Drug Pricing Program contract pharmacy services and support for the upcoming Department of Health and Human Services, Health Resources and Services Administration (HRSA) audit.</td>
<td>Request for retroactive approval and overview of engagement will be brought to the JACC at their June 2019 meeting.</td>
</tr>
</tbody>
</table>
TO: Members of the Joint Audit & Compliance Committee

FROM: Cheryl Chiaputti  
Chief Audit Executive

DATE: June 19, 2109

SUBJECT: Appointment of Vizient Inc. to Provide Audit Services

RECOMMENDATION

That the JACC retroactively approve the appointment of Vizient, Inc to conduct an audit of the UConn Health’s John Dempsey Hospital (JDH) 340B Drug Pricing Program contract pharmacy services and to provide support for an upcoming audit that will be conducted by the Department of Health and Human Services, Health Resources and Services Administration (HRSA). The total fee for this engagement is $30,059, which includes project-related reimbursable expenses for administrative costs. The engagement term is January 2019 through June 2019.

BACKGROUND

As a 340B covered entity, JDH has elected to dispense 340B drugs to patients through contract pharmacy arrangements.

Federal Register Vol. 75, No. 43 Notice Regarding 340B Drug Pricing Program — Contract Pharmacy Services issued guidelines that govern the operation and compliance of contract pharmacies for 340B covered entities. These guidelines require that “Covered entities are responsible for ensuring compliance of their contract pharmacy arrangement(s) with all 340B Program requirements. In order to fulfill the ongoing obligation of compliance, all covered entities are required to provide oversight of the contract pharmacy, maintain auditable records and are expected to conduct annual audits of their contract pharmacies, completed by an independent auditing firm”.

The engagement with Vizient, Inc. is designed to fulfill the audit requirement. The Office of Audit and Management Services seeks JACC approval of this engagement.

Approved by the Joint Audit & Compliance Committee at their _________ meeting
THIS PAGE INTENTIONALLY LEFT BLANK
University of Connecticut
&
University of Connecticut Health Center

Joint Audit & Compliance Committee Meeting
University of Connecticut
Single Audit Report Excerpts
FYE 6/30/2018

- Issue Date – March 28, 2019

The audit was performed in accordance with auditing standards generally accepted in the United States of America, Government Auditing Standards for financial audits issued by the Comptroller General of the United States, and the audit requirements of Title 2 U.S. Code of Federal Regulations Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance)

- Complete Statewide Report -

- Applicable University Federal Programs
  1) Research and Development
  2) Federal Student Financial Assistance (FSFA)
Federal Funds

- Total Federal Assistance Statewide - $9,821,000,000

Type A Program Threshold

(<$10B = Larger of $3m or FFA * .003) - $29,463,000

- Federal Assistance Expended at the University System:
  1. University R&D $ 89,500,000
  2. Health Center R&D $ 63,300,000
  3. Student FFA $230,600,000 (Storrs $213.2m UCHC $17.4m)

  TOTAL FFA $383,400,000
Audit Findings – R&D

1. Reporting (University) 2018-500

- Title 2 Code of Federal Regulations (CFR) Part 200.327, requires the submission of federal financial reports in the manner specified by the Office of Management and Budget.

- Title 2 CFR Part 1800.906 states that “The recipient shall submit a Federal Financial Report (SF-425) electronically to the Department of Health and Human Services/Payment Management System within 30 days following the end of each federal fiscal quarter.”

Our review of federal financial reports disclosed one report in which the University of Connecticut overstated cumulative cash disbursements by $19,116. Further review disclosed multiple invoices since 2016 with overpayments totaling $75,677. The Accounts Payable Department processed multiple vendor invoices using the amount in the invoice’s cumulative amount column instead of the current amount billed. The university resolved these overpayments as of October 19, 2018, as reflected in the SF-425 it submitted for December 31, 2018.

Agency Response – “Management concurs with this recommendation”
Audit Findings - FSFA

2. Activities Allowed or Unallowed (University) 2018-650

- Title 34 Code of Federal Regulations 675.9 states that a student at an institution of higher education is eligible to receive part-time employment under the Federal Work Study program for an award year if the student is enrolled at the institution.

From a sample of 12 students who received Federal Work Study and separated from the university, we noted 2 instances in which students received Federal Work Study funds for work performed after separation.

*Agency Response – “We agree with this finding.”*
3. Special Tests: Student Loan Repayments – Default (University) 2018-655

- Title 34 Code of Federal Regulations 674.42(c) requires that an institution must contact a federal Perkins Loan borrower with a 9-month grace period at the 90-day, 150-day, and 240-day points of the grace period.

- The Federal Student Aid Handbook states, “Initial grace period – a nine-month period that immediately follows a period of enrollment and immediately precedes the date repayment is required to begin for the first time.” The Handbook further states, “The borrower is entitled to a full initial grace period (nine consecutive months) from the date that he or she graduates, withdraws, or drops below half-time enrollment again.”

During our review of 10 borrowers at the university whose loans went into default during the audited period, we noted that the university did not send all of the required grace letters to the borrowers in a timely manner. The letters were sent between 5 and 8 days late.

*Agency Response – “We agree with this finding.”*
UNIVERSITY OF CONNECTICUT

2018-500  Reporting (University of Connecticut)

Federal Award Agency: National Aeronautics and Space Administration
Award Year: State Fiscal Year Ended June 30, 2018
Research and Development Programs:
  Aeronautics (CFDA 43.002)
    Account # 5635240 – “Reduced kinetic models with fuel sensitivity for turbulent combustion simulations” – NNX15AU96A, project period December 1, 2015 through May 31, 2019

Criteria:  Title 2 Code of Federal Regulations (CFR) Part 200.327, requires the submission of federal financial reports in the manner specified by the Office of Management and Budget.

Title 2 CFR Part 1800.906 states that “The recipient shall submit a Federal Financial Report (SF-425) electronically to the Department of Health and Human Services/Payment Management System within 30 days following the end of each federal fiscal quarter.”

Instructions for the preparation of the SF-425 report require the recipient to enter cumulative amounts of cash receipts and disbursements from the inception of the award through the end date of the reporting period on the report.

Condition:  Our review of federal financial reports disclosed one report in which the University of Connecticut overstated cumulative cash disbursements by $19,116. Further review disclosed multiple invoices since 2016 with overpayments totaling $75,677. The Accounts Payable Department processed multiple vendor invoices using the amount in the invoice’s cumulative amount column instead of the current amount billed. The university resolved these overpayments as of October 19, 2018, as reflected in the SF-425 it submitted for December 31, 2018.

Context:  These errors appear to be isolated, relating to the application of a negative expense to a grant account for the overpayment of invoices to a subgrantee.

We reviewed federal financial reports filed for 10 federal research and development awards. The Schedule of Expenditures of Federal Awards reflects activity in 1,322 University of Connecticut federal research and development accounts. In some instances, the university may maintain multiple accounts for the same award. Our sample was not statistically valid.

Questioned Costs:  $0
Auditors of Public Accounts

**Effect:** SF-425 Federal Financial Reports did not accurately reflect the financial status of the program.

**Cause:** The university paid the incorrect amount on several subaward invoices, which overstated disbursements and the amount reported on the federal financial report.

**Prior Audit Finding:** We have not previously reported this finding.

**Recommendation:** The University of Connecticut should strengthen internal controls to ensure that it reports accurate amounts on federal financial reports.

**Views of Responsible Officials:**

“Management concurs with this recommendation. Sponsored Program Services has internal controls in place in which all quarterly financial reports receive secondary review and the preparer of the financial report and the certifier of the financial report are separate individuals. Additionally, multiple review and approval levels are required for all expenditures. As noted above, this was an isolated occurrence. However to further strengthen internal controls, Accounts Payable will implement additional procedures and notifications to provide Sponsored Programs Services with timely information of any overpayment that impacts the accuracy of amounts reported on federal financial reports. Additionally, focused training is being provided to the individuals involved in this transaction and broad training will be provided to faculty and staff.”
2018-650  Activities Allowed or Unallowed

Federal Work Study (CFDA 84.033)
Federal Award Agency: United States Department of Education
Award Year: 2017-2018

Criteria: Title 34 Code of Federal Regulations 675.9 states that a student at an institution of higher education is eligible to receive part-time employment under the Federal Work Study Program (FWS) for an award year if the student is enrolled at the institution.

Condition: We selected a sample of 12 students who received Federal Work Study and also separated from the University of Connecticut (UConn). From this sample, we noted 2 instances in which a student received Federal Work Study funds for work performed after their separation. In the first instance, the student separated on March 29, 2018, but their timesheet reflected that they worked between April 2, 2018 and April 12, 2018. In the second instance, the student separated on November 8, 2017, but their timesheet reflected that they worked on December 22, 2017. In each instance, the student was paid with Federal Work Study funds. When we brought these matters to the university’s attention, they returned the funds to the Federal Work Study Program.

Context: UConn awarded Federal Work Study to 990 students during the audited period. We identified 17 students who were awarded Federal Work Study and subsequently separated from the University. We selected 12 for testing. The sample was not statistically valid.

Questioned Costs: $0

Effect: The university paid students with Federal Work Study funds for work performed after their separation.

Cause: The university normally contacts the student’s supervisor when a Federal Work Study recipient withdraws to prevent them from being paid after their separation. In these instances, the procedure was not followed.

Prior Audit Finding: We have not previously reported this finding.

Recommendation: The University of Connecticut should ensure that students do not get paid from Federal Work Study funds for work they performed after their separation.

Views of Responsible Officials: “We agree with this finding. The staff member responsible for the procedure has been notified and has been following the procedure moving forward. In addition, internal controls have been enhanced to include additional steps to
Auditors of Public Accounts  

the Federal Work Study reconciliation and student separation procedures. An additional staff member has also been added to the internal control process for quality assurance purposes and has been conducting an internal review throughout the academic year.”

2018-651 Cash Management

Federal Direct Student Loans (CFDA 84.268)
Federal Award Agency: United States Department of Education
Award Year: 2017-2018

Criteria: Title 34 CFR 668.166(b) states that an institution may maintain an amount of excess cash for up to 7 days that does not exceed 1 percent of the total amount of funds the institution drew down in the prior award year. The institution must immediately return any amount of cash over the 1 percent tolerance and any amount remaining in its account after the 7-day tolerance period to the Secretary of the US Department of Education.

Condition: Western Connecticut State University (Western) held excess Direct Loan funds longer than allowed. The university held Direct Loan funds totaling $98,622 for 9 days, 2 days beyond the allowable 7-day period.

Manchester Community College (Manchester) held excess Direct Loan funds longer than allowed. The college held Direct Loan funds totaling $1,992 and $761 for 11 and 14 days, respectively. The 11 and 14 days are 4 and 7 days beyond the allowable 7-day period.

Context: Western: The condition appears to be an isolated instance. The university made 35 Direct Loan drawdowns, totaling $28,597,256, during the 2017-2018 award year. The sample was not statistically valid.

Manchester: The condition appears to be an isolated instance. The college made 10 Direct Loan drawdowns, totaling $543,367, during the 2017-2018 award year. The sample was not statistically valid.

Questioned Costs: Western and Manchester: $0

Effect: These institutions did not comply with established cash management procedures.

Cause: Western: It appears the delay was caused, in part, by a holiday occurring during the excess cash period.

Manchester: The timeliness of processing adjustments in students’ accounts caused these delays.
Prior Audit Finding: We have not previously reported this finding at these institutions.

Recommendation: Western Connecticut State University and Manchester Community College should comply with federal cash management requirements by ensuring that any excess cash is returned within the timeframe established in the regulations.

Views of Responsible Officials:
Western: “We agree with this finding. WCSU will ensure that disbursements are scheduled with time enough to allow for a timely adjustment by the Fiscal Affairs office.”

Manchester: “We agree with this finding. The college reviewed the 2 instances where loan funds were held longer than the 7-day period. The Director of Financial Aid, the Director of Administrative Affairs/Finance and Administrative Services, and the Dean of Student Affairs met to discuss the error of the delay in returning the funds. The Director of Administrative Affairs/Finance and Administrative Services has reviewed the policy and procedure with the appropriate staff, and measures are in place to prevent reoccurrence, and comply with the regulation.”

2018-652 Special Tests – Disbursements

Federal SEOG (CFDA 84.007)
Federal Work-Study (CFDA 84.033)
Federal Perkins Loans – Federal Capital Contributions (CFDA 84.038)
Federal Pell Grant Program (CFDA 84.063)
Federal Direct Student Loans (CFDA 84.268)
Federal Award Agency: United States Department of Education
Award Year: 2017-2018

Criteria: 34 CFR 668.164(h)(2) requires that a credit balance in a student’s account must be paid to the student within 14 after the balance occurred.

Condition: We selected 10 Title IV recipients from Manchester Community College for disbursements testing. From this sample, we noted 4 instances during the spring 2018 semester in which the college did not pay the student a credit balance resulting from the disbursement of Title IV funds within the required timeframe. The college paid the students’ credit balances between $21 and $952 3 days late.

Context: The college made over 3,000 disbursements, totaling over $9 million in federal aid, during the award year. The sample was not statistically valid.
**Questioned Costs:** $0

**Effect:** The college did not pay credit balances to students in a timely manner.

**Cause:** A change in staffing resulted in the credit balances being paid late.

**Prior Audit Finding:** We have not previously reported this finding.

**Recommendation:** Manchester Community College should pay credit balances resulting from Title IV program receipts directly to the student within the required timeframe.

**Views of Responsible Officials:**

“We agree with this finding. The college reviewed the 4 instances where Title IV funds were not returned within the required 14 days. The Director of Financial Aid, the Director of Administrative Affairs/Finance and Administrative Services, and the Dean of Student Affairs met to discuss the error of the delay in returning funds. The Director of Administrative Affairs/Finance and Administrative Services has reviewed the policy and procedure with the appropriate staff, and measures are in place to prevent reoccurrence, and comply with the regulation.”

---

**2018-653 Special Tests – Return of Title IV Funds**

**Federal Supplemental Educational Opportunity Grants (CFDA 84.007)**
**Federal Perkins Loan - Federal Capital Contributions (CFDA 84.038)**
**Federal Pell Grant Program (CFDA 84.063)**
**Federal Direct Student Loans (CFDA 84.268)**
**Federal Award Agency: United States Department of Education**
**Award Year: 2017-2018**

**Criteria:** Title 34 Code of Federal Regulations 668.22 details requirements regarding the treatment of Title IV funds when a student withdraws from an institution.

Title 34 CFR 668.22(f) states that the percentage of the payment period or period of enrollment completed is determined by dividing the total number of calendar days in the payment period or enrollment period into the number of calendar days completed in the period as of the student’s withdrawal date. In addition, Dear Colleague Letter GEN 11-14 provides guidance on handling summer session withdrawals. It states, for summer sessions, where the payment period is the term comprising both sessions, all students who withdraw are considered to be withdrawing from a program offered in modules.
Title 34 CFR 668.22(j) states that an institution must return the amount of Title IV funds for which it is responsible as soon as possible but no later than 45 days after the date the institution’s determination that the student withdrew.

**Condition:**

From a sample of 10 students who we selected for Return of Title IV Funds testing at Central Connecticut State University (Central), we identified 2 instances in which the university did not correctly calculate the return of Title IV funds. Each instance resulted in an excess return of Title IV funds. One was to the Pell Grant Program for $25, and the other was to the Direct Loan Program for $310.

Our review of Return of Title IV Funds calculations at Eastern Connecticut State University (Eastern) revealed that the university used the incorrect enrollment period when calculating returns for the summer 2018 term. As a result, the university performed 2 return calculations inaccurately. In each instance, the university over returned Pell Grant funds.

From a sample of 10 students who we selected for Return of Title IV Funds testing at Western Connecticut State University (Western), we noted an instance in which the university improperly excluded several adjustments to a student’s meal plan charges in calculating institutional charges. This resulted in an over return of $94 to the Federal Direct Student Loans Program.

From a sample of 10 students selected for Return of Title IV Funds testing at Manchester Community College (Manchester), we noted the following:

- The college used the incorrect enrollment period when calculating the spring 2018 return calculations. The college used 112 days, instead of the correct 109 days.
- In 2 instances, the college did not return Title IV funds in a timely manner. The college returned the funds between 3 and 8 days late.

From a sample of 5 students who we selected for Return of Title IV Funds testing at Tunxis Community College (Tunxis), we noted the following:

- In 2 instances, the college did not return Title IV funds in a timely manner. The college returned funds between 10 and 20 days late.
- In 2 instances, the college did not correctly calculate the return of Title IV funds. One instance resulted in a $21 under return of Title IV funds to the Pell Grant Program, and the other a $79 under return to the Direct Loan Program.

**Context:**

None of the samples were statistically valid.

*Central:* The university performed 2 Return of Title IV Funds calculations during the 1st summer session of 2018 and used the incorrect enrollment period for both calculations.
Eastern: The university performed 2 Return of Title IV Funds calculations during summer 2018 and used the incorrect enrollment period in each instance.

Western: The university performed 76 Return of Title IV Funds calculations during the audited period.

Manchester: The first issue is systemic. The college performed 95 Return of Title IV Funds calculations for the spring 2018 semester. The second issue does not appear to be a systemic issue. The college performed a total of 199 Return of Title IV Funds calculations during the audited period.

Tunxis: The college performed 49 Return of Title IV Funds calculations during the audited period. Based on discussions with college staff and our review, this condition does not appear to be systemic. We brought this matter to the attention of college officials and they corrected the matter.

**Questioned Costs:** $0

**Effect:** The colleges and universities delayed or improperly calculated Title IV funds that were due to be returned to the U.S. Department of Education.

**Cause:**

*Central:* This was caused by a clerical error when determining the enrollment period.

*Eastern:* This was caused by the university’s incorrect interpretation of the number of days in the summer session.

*Western:* It appears that there was a clerical error in calculating institutional charges.

*Manchester:* For the first item, the college did not accurately adjust the spring 2018 break period from the enrollment period. For the second item, delays in performing refund calculations caused the delay in returning the funds.

*Tunxis:* Delays in performing the refund calculations attributed to delays in returning the funds. There were clerical errors when entering enrollment period and institutional charges.

**Prior Audit Finding:** Central, Western, and Manchester: We have not previously reported this finding.

*Eastern:* We previously included a Return of Title IV Funds finding as 2017-653; however, that was not the same condition noted in the current audit.

*Tunxis:* We previously reported this as finding 2017-653.
Recommendation: The colleges and universities should review their procedures to ensure compliance with the federal regulations contained in 34 CFR 668.22. In addition, Eastern Connecticut State University should comply with the requirements contained in Dear Colleague Letter GEN 11-14 when determining enrollment periods to be used in Return of Title IV Funds calculations.

Views of Responsible Officials:

Central: “We agree with this finding. To mitigate the risk of future errors, the Financial Aid Office will rely on the term dates listed in Banner STVTERM and SOATERM tables when completing return of Title IV funds. The Registrar’s Office has confirmed that these tables always reflect the most current dates. In addition, the Registrar’s Office will advise the Financial Aid Office of any changes to the published academic calendar. The two students in question regarding this finding had their R2T4’s recalculated and properly documented on August 23, 2018.”

Eastern: “We do not agree with this finding. According to the Federal Student Aid Handbook ‘In determining the percentage of the payment period or period of enrollment completed for a student who withdraws from a program offered in modules, the school includes in the denominator (the total number of calendar days in the payment period or period of enrollment) all days within the period that the student was scheduled to complete (including those completed by the student) prior to ceasing attendance, excluding days in which the student was on an approved leave of absence and excluding any scheduled breaks of at least five consecutive days when the student was not scheduled to attend a module or other course offered during that period of time.’

As the federal student handbook was published after the GEN-11-14 DCL, we find the most recent publication to be the most accurate.”

Western: “We agree with this finding. This was clerical error in nature.”

Manchester: “We agree with this finding. The college reviewed the 95 return calculations for Spring 2018, based on the incorrect days in Banner for the Spring break period. The Director of Financial Aid, the Registrar, and the Dean of Student Affairs met to discuss the error in the Spring break period. The Registrar has reviewed the policy and procedure, and measures are in place to prevent reoccurrence and comply with the regulation.

The college reviewed the 2 instances where Title IV funds were not returned within the required 45 days, since the students withdrew from all classes. The Director of Financial Aid has reviewed the policy and procedure with the appropriate staff, and measures are in place to prevent reoccurrence and comply with the regulation.”
Tunxis: “We agree with this finding. The Director of Financial Aid reviewed the federal regulations contained in 34 CFR 668.22. An electronic monthly calendar will be created by the DFA. The Associate Director of Financial Aid will refer to the calendar to complete the Return of Title IV funds each semester. The DFA will check all returns one week prior to the deadline date that the Title IV refunds should be returned to the DOE.

As for the clerical errors made, the DFA will review all R2T4 calculations entered by the ADFA before any funds are returned.

The DFA will meet the Registrar to create a schedule to run the withdrawal reports on a weekly basis. This will ensure that we complete the R2T4 process in a timely manner.”

Auditors’ Concluding Comments:

The section of the Federal Student Aid Handbook that officials at Eastern cited is more general and does not closely relate to the unique situation at the university. In our opinion, Dear Colleague Letter GEN 11-14 is more directly related to withdrawals during the summer sessions at Eastern.

In addition, in its corrective action plan, the university expressed a willingness to change its procedures to review summer withdrawals using individual modules. This revision would bring the college into compliance with Dear Colleague Letter GEN 11-14.

2018-654 Special Tests – Enrollment Reporting

Federal Perkins Loans – Federal Capital Contributions (CFDA 84.038)
Federal Pell Grant Program (CFDA 84.063)
Federal Direct Student Loans (CFDA 84.268)
Federal Award Agency: United States Department of Education
Award Year: 2017-2018

Background: The National Student Loan Data System (NSLDS) is the United States Department of Education’s central database for federal student aid disbursed under Title IV of the Higher Education Act of 1965, as amended. NSLDS monitors the programs of attendance and the enrollment status of Title IV aid recipients.

Criteria: Title 34 Code of Federal Regulations 685.309(b)(2), requires changes in enrollment to less-than-half-time, graduated, or withdrawn, must be reported within 30 days. However, if a roster file is expected within 60 days, the data may be provided on that roster file.
The NSLDS Enrollment Reporting Guide outlines the specific enrollment reporting requirements, including the valid enrollment status codes that each institution must use when reporting enrollment changes. A school must correctly report students who have completed a program as “graduated” and not as “withdrawn.”

**Condition:** We selected 10 students who separated during the audited period from Southern Connecticut State University. We noted 2 instances in which the university incorrectly reported the students’ enrollment information to the NSLDS. In these instances, the university did not update the students’ enrollment status to reflect each student’s graduation.

**Context:** Based on the university’s response, the condition does not appear to be a systemic issue. The university reported 1,120 students who graduated during the 2017-2018 award year. Our sample contained a total of 10, 5 of whom were reported as having graduated. Our sample was not statistically valid.

**Questioned Costs:** $0

**Effect:** The university did not provide enrollment information to the NSLDS for these students in an accurate manner.

**Cause:** The university did not follow established procedures for reporting enrollment changes. In the first instance, the university did not report the student’s degree award to its third-party service provider. In the second instance, while the university reported the degree award, it was never applied to the students account because the student received two degrees and the university did not verify that the status was applied to the correct program(s).

**Prior Audit Finding:** We previously reported this as finding 2017-654.

**Recommendation:** Southern Connecticut State University should review its procedures to ensure that enrollment status changes are accurately submitted to the NSLDS in accordance with federal regulations.

**Views of Responsible Officials:**

“We agree with this finding. To ensure enrollment reporting occurs for students retroactively awarded for prior terms, the procedures have been revised effective October 2018. The Registrar’s Office has added additional degree file transmissions to ensure late awards are captured and reported. The monthly degree file transmission will now include the 4 most recently completed terms of fall, winter, spring, and summer, not only last completed term. This will serve as a back up to our standard late award procedures, while ensuring timely reporting.”
In addition, the National Student Clearinghouse provides a report following each degree file transmission called ‘G Not Applied’. This includes students graduating from multiple programs who require manually verification of the graduation status. The procedures were updated to ensure that these files are reviewed and reconciled within 1-2 weeks following each degree transmission. Training with the staff was performed and these reconciliation activities will continue to be monitored by a supervisor to ensure regular completion and provide back up when necessary.”

2018-655  Special Tests – Student Loan Repayments - Default

Federal Perkins Loan – Federal Capital Contributions (CFDA 84.038)
Federal Award Agency: United States Department of Education
Award Year: 2017-2018

Criteria: Title 34 Code of Federal Regulations 674.42(c) requires that an institution must contact a federal Perkins Loan borrower with a 9-month grace period at the 90-day, 150-day, and 240-day points of the grace period.

The Federal Student Aid Handbook states, “Initial grace period – a nine-month period that immediately follows a period of enrollment and immediately precedes the date repayment is required to begin for the first time.” The handbook further states, “The borrower is entitled to a full initial grace period (nine consecutive months) from the date that he or she graduates, withdraws, or drops below half-time enrollment again.”

Condition: We selected 10 borrowers at the University of Connecticut whose loans went into default during the audited period and noted that the university did not send all of the required grace letters to the borrowers in a timely manner. The letters were sent out between 5 and 8 days late.

Context: Based on the exception percentages and discussions with university staff, these findings appear to be systemic. The mailing of grace letters is delayed due to a discrepancy in the start dates of the grace period. The university provided us a report of 82 borrowers whose loans went into default during the audited period. Our sample was not statistically valid.

Questioned Costs: $0

Effect: The university was not in compliance with the federal due diligence requirements designed to minimize repayment defaults.
Cause: The university’s third-party Perkins Loans servicer uses the first day of the following month to start the billing cycle for student loans. Grace letters are based on this date, rather than on the actual start date.

Prior Audit Finding: We previously reported this as finding 2017-656.

Recommendation: The University of Connecticut should ensure that policies and procedures related to Perkins Loans due diligence requirements are being performed in accordance with federal regulations.

Views of Responsible Officials:
“We agree with this finding. The ten instances identified in which one or more of the required grace letters were not sent in a timely manner are associated with the timing of the billing cycle of the University’s third party servicer. Such instances are related to a finding identified in the FY16-17 audit. As the University responded in the FY16-17 audit, the third party servicer had established their repayment date as the first subsequent month following the expiration of the grace period. Grace period notification were sent when the billing calculation occurred rather than based upon the specific separation date.

When the University reached out to the third party service provider in October, 2017, the third party service provider was reluctant to change procedures that had been audited annually by the Department of Education without exception. In December, 2017, the University reached out to DOE to confirm that the third party service provider’s practices were compliant with federal regulations. Upon further review, the DOE concluded that the University’s third party service provider was not compliant with Title 34 Code of Federal Regulations 674.42(c). The DOE recommended that the third party service provider align its practices with the state auditor’s recommended practice. In addition, the DOE confirmed that because the third party service provider had not received prior audit findings specific to this regulation, institutions using this provider, as well as the provider, would be held harmless for this past practice.

The DOE has confirmed, effective May 2018, the third party service provider implemented changes to its grace expiration notice process. Upon corrective action taken by the third party service provider, the University does not anticipate future findings specific to Title 34 Code of Federal Regulations 674.42(c).”
THIS PAGE INTENTIONALLY LEFT BLANK
SIGNIFICANT COMPLIANCE ACTIVITIES

**Faculty and Staff Training** – The Office of University Compliance (OUC) achieved a 100% completion rate for this year’s Annual Compliance Training. Additionally, in an effort to continue to build commitment and understanding of responsibilities regarding compliance-related matters and ethical leadership, OUC is working on revamping its management development module at UConn Health. We anticipate launching in the Fall of 2019.

**Investigations** – As of June 3rd, OUC has received 71 reports through the REPORTLINE. UConn Health accounts for approximately 40% of all reported concerns.

**Education and Awareness** - OUC hosted a Compliance Network event at UConn Health on April 30th. Various departments with compliance responsibilities were represented. Per survey results the event was well received and successful. The next Compliance Network event will be held in Storrs and is scheduled for November 2019.

OUC presented to multiple populations at UConn Health in an effort to continue to educate the community and raise awareness regarding compliance-related matters. OUC partnered with various areas across UConn and UConn Health in the development of education and awareness materials related to a number of compliance topics, including rules related to foreign affiliations, the employment of international students, use of University funds, the protection of minors on campus, and faculty consulting.

**Healthcare and Regulatory Compliance Restructuring** - Last year in conjunction with the reorganization of the Audit, Compliance and Privacy functions for the University, a separate Clinical Compliance function was created at UConn Health that consolidated Regulatory and Compliance staff. Following a recent review, it has been concluded that having separate Regulatory and Compliance functions best serve the complex needs of the clinical enterprise.

Deb Abromaitis, who has been serving as the Interim Compliance Officer, has agreed to take the role of Director of Clinical Regulatory Compliance. In this role she will assume expanded responsibilities for Regulatory activity for all clinical operation. Strong collaboration on quality and patient safety will also be an important priority in this position.

A search is currently underway for a Director of Clinical Compliance who will be responsible for developing, implementing and monitoring UConn Health’s clinical compliance programs.
SIGNIFICANT COMPLIANCE ACTIVITIES

Healthcare and Regulatory Compliance

Overpayment

The Office of Healthcare and Regulatory Compliance (OHRC) has been working with Finance to follow up on any potential overpayment concerns. No overpayments were refunded.

National Government Services

OHRC is continuing education and monitoring for identified Targeted Probe and Educate (TPE) reviews.

Regulatory Visits

This quarter continued with regulatory surveys of the clinical areas. The Joint Commission (TJC) certified John Dempsey Hospital as a Primary Stroke Center with Endovascular capabilities in January 2019. Our Stroke Program has been notified that we received the 2019 Get with the Guideline Gold Plus and Target Stroke Elite Plus Award (the highest award possible).

We were surveyed by the American Heart Association’s Mission Lifeline. The American Heart Association accredited UConn Health’s John Dempsey Hospital as a Heart Attack Receiving Center. We are the first in the state to achieve this accreditation. In addition, John Dempsey Hospital was re-certified by the Center of Excellence for Minimally Invasive Gynecological Surgery. Five Surgeons qualified as Surgeons specializing in these specialty procedures.

We participated in a webinar with The Joint Commission as a follow up to a sentinel event. We are auditing and monitoring the corrective action plan.

The office continues to work towards accreditation as a Level 3 Trauma program.

We continue to monitor all corrective actions, update and provide guidance materials and support for all areas for regulatory preparedness and response.
Dear Members of the University Community,

UConn is deeply committed to international collaborations, interdisciplinary research, and global exchange of ideas, students, and scholars. Our global collaborations enrich our University and are integral to providing the highest quality education, outreach, research, and patient care.

As you may be aware, the federal government is actively examining foreign influences on federally funded research and expressed concerns about foreign threats to research at U.S. universities. Over the last year, congressional leaders and several federal agencies have issued statements outlining these concerns. Statements have been issued by the National Institutes of Health (NIH), the National Science Board (NSB/NSF), the Department of Defense, and the Department of Energy regarding concerns about:

1) diversion of intellectual property,
2) failure to disclose financial support and resources,
3) duplication of research programs and funding,
4) breaches in scientific integrity, and
5) threats to national security and economic competitiveness

All faculty, principal investigators, and research staff with sponsored funding must be aware of and follow all sponsor rules and regulations, and should be mindful of the following:

**Transparency in Disclosure**

- Be thorough and complete in disclosing and accounting for all forms of research support, whether or not that funding is passed through the University. Forms of research support include financial support and resources from funding agencies, other institutions, and foreign entities (e.g., active and pending support included in grant applications and prior to award issuance).
- Foreign components of federally funded research must be disclosed and approved in advance by the sponsor.
- Significant financial interests such as equity in a publicly or non-publicly traded entity, salary support outside of UConn, or any remuneration such as income from consulting, honoraria, or paid authorships must be disclosed annually and may require prior approval.
- Extramural professional activities, whether compensated or uncompensated, should be disclosed through the consulting approval process to determine if there are potential conflicts of interest or commitment.

Additional guidance is available from the Office of the Vice President for Research (OVPR) on several of these topics including: active and pending support, foreign components, export controls, and disclosure of financial interests. The OVPR will also implement additional trainings and outreach to assist faculty and principal investigators in these and any related matters.
UConn is committed to supporting our innovative faculty, students, and staff to promote global exchange and collaboration, while at the same time providing the University community with the necessary information to ensure the integrity of our research. It is critically important that the entire University demonstrate leadership in research and in our shared responsibility to be accountable, compliant, and mitigate risk.

Distributed via email April 25, 2019
International Relationships, Foreign Components, & Sponsored Programs

April 8, 2019
The University both encourages and works to facilitate international collaborations.

- Especially in the context of multidisciplinary research and sponsored program activities

However, it is important that faculty and investigators are transparent in disclosing these relationships to the University and funding agencies.

- Allows the University and sponsors to determine if there are any potential conflict of interest and commitment, duplication of research, need to adjust funding, and/or diversion of intellectual property from federally funded research
These expectations and requirements regarding disclosure are not new and have been in place for a number of years.

More recently, serious and growing concerns have been raised by federal funding agencies regarding nondisclosure of foreign affiliations and “systemic programs” of influence from foreign entities on federally funded research.
Office of the Vice President for Research

• August 20, 2018, memo from NIH Director Francis Collins stating that the failure to properly disclose foreign relationships threatens to distort decision-making about the use of NIH funds.

• October 23, 2018, the National Science Board which oversees the National Science Foundation (NSF) released a statement that U.S. universities must “embrace transparency and rigorously adhere to conflict of interest and conflict of commitment policies.”

• December 13, 2018 NIH Advisory Committee to the Director identified 3 areas of concern: undisclosed foreign financial conflicts, undisclosed conflicts of commitment, and peer review violations.
August 13, 2018, the National Defense Authorization Act included provisions that academic institutions that perform defense research and engineering activities act to. . .”limit undue influence, including through foreign talent programs, by countries to exploit United State Technology ... “

• “limit or prohibit funding...for institutions or individual researchers who knowingly violate regulations...”

February 1, 2019, the Department of Energy (DOE) issued a notification that it will implement a policy, which will mandate that “federal and contractor personnel fully disclose and, as necessary, terminate affiliations with foreign government-supported talent recruitment programs.”
Vast majority of international collaborations are appropriate, acceptable, and meet compliance requirements; however, there have been several high profile exceptions:

- In 2006, University of Tennessee professor sentenced to four years in prison for violating US export control laws regarding foreign nationals working on restricted research.
- In 2010, FBI launches investigation of a former exchange student accused of stealing intellectual property from federally funded research conducted at Duke University.
- In 2014, three NYU researchers arrested and indicted on fraud and conspiracy charges regarding NIH grants and undisclosed foreign financial affiliations. One pled guilty, one had charges dropped, and third left the U.S.
- In 2019, Virginia Tech Professor found guilty of grant fraud by federal court. Submitted grant applications to NSF and DOE for research already completed and supported by a foreign funding agency.
What is expected to be compliant with receiving federally funded research?

- Foreign components of federally funded research must be disclosed and approved formally by the sponsor prior to engaging the foreign component.
  - Include the component in the proposal submitted to the sponsor (current/pending) or make a formal request of the sponsor through Sponsored Program Services.
- The NIH defines foreign components as “any significant scientific element or segment of a project outside of the United States, either by the recipient or by a researcher employed by a foreign organization, whether or not grant funds are expended.”
  - May include “collaborations with investigators at a foreign site anticipated to result in co-authorship; use of facilities or instrumentation at a foreign site; or receipt of financial support or resources from a foreign entity.”
- Other sponsors have similar requirements.
What is expected to be compliant with receiving federally funded research?

- Disclosure of all Significant Financial Interests which includes such things as equity in a publicly traded entity (at least 5% interest or $5000), or other compensation including salary, consulting fees, honoraria, or paid authorship

- The NIH is expected to release additional guidance in April regarding disclosure requirements for foreign affiliations and what constitutes foreign components.
What has occurred at UConn?

- NIH issued letters to several universities regarding potential nondisclosure of foreign components of NIH-funded research for investigators at the respective institutions. UConn was among the universities notified.

- In addition, other faculty not identified by NIH have contacted the OVPR to discuss their foreign collaborations.

- The OVPR has worked with identified faculty to assess whether there is or is not a foreign component to their funded research, whether disclosure should have occurred, and if necessary, to take corrective action.
What has occurred at UConn?

• Corrective actions may include notifying the funding agency to ensure compliance, providing additional training, correcting grant reports, correcting publications, notifying relevant University committees (i.e., Financial Conflict of Interest in Research Committee, Faculty Consulting Committee), and adjusting awards if required by the funding sponsor.

• Depending on the circumstance, failure to disclose all relationships could result in the termination of funding for a project and potential ineligibility for future funding.

• Noncompliance can threaten not only the funding for individual projects, but overall funding for the University as a whole.
What should faculty do if they have concerns/questions?

• Contact the OVPR
  • Laura Kozma, Executive Director SPS (laura.Kozma@uconn.edu)
  • Paul Hudobenko, Director SPS—UCH (hudobenko@uchc.edu)

• The OVPR will determine if there is a foreign component and if disclosure is required. The OVPR will then provide the appropriate guidance and implement corrective actions as necessary.
University of Connecticut & University of Connecticut Health Center

Joint Audit & Compliance Committee Meeting
UConn Joint Audit and Compliance Committee Meeting:
HealthONE Update

Bruce A. Metz, Ph.D.
Vice President and Chief Information Officer, UConn Health

June 19, 2019
HealthONE Update: Stabilization Summary

Notable Successes

- The one-year mark since the April 28, 2018 go-live was reached with impressive outcomes such as:
  - 2.2 million inpatient orders have been processed
  - About 790,000 outpatient appointments were scheduled
  - Approximately 35,000 ED visits were conducted
  - Revenue in excess of $318 million was posted based on 432,000 claims
- Progress continues to be made stabilizing the Epic system in key clinical, operational and revenue cycle areas
  - Over 60 projects addressing a range of Epic system and operational issues have been completed
  - Some focused efforts to resolve departmental problems and challenges such as in Dermatology were finished according to plan
  - 95 percent of nearly 35,000 service desk calls have been resolved
  - More than 1,200 instructor led classes have been held providing essential training to thousands of attendees
- Important, new capabilities have been deployed over the past several months, particularly:
  - A “reboot” of Epic’s patient portal along with a name change to “myUConnHealth” was completed
  - Kaleidoscope, Epic’s Ophthalmology module which was not part of the initial implementation, went live
  - HeathData Archiver, a software solution to store and easily retrieve patient information in legacy EMRs such as NextGen, was rolled out
- Virtually all consulting resources have been rolled off placing greater emphasis of Epic system ownership on UConn Health staff
- An operationally driven project prioritization framework has been put in place to help ensure alignment of the work plan, resource levels, and UConn Health goals
- A major project to upgrade the Epic system to a current release (e.g., Version 2018) has started and is in the detailed planning phase

Major Concerns and Outstanding Issues

- Enterprise-wide adoption of Epic’s integrated and standardized ways of working represents a dramatic change and ongoing learning curve
- Various workflows remain challenging to perform, particularly in clinical areas, necessitating broad remediation efforts
- Common processes across the organization such as internal/external referrals require redesign and an optimization strategy
- Over 90 stabilization projects that have been defined, as well as enhancement requests and strategic initiatives, will be difficult to undertake until the upgrade project is completed given current staff resource levels

Key Next Steps

- Complete planning for the upgrade project and begin system build phase by July with go-live targeted for early December, 2019
- Move ahead with the project prioritization framework and expand other governance groups to foster greater stakeholder involvement
- Continue the project rebranding process by simplifying the internal name, changing from “HealthONE” to “Epic”
University of Connecticut
&
University of Connecticut Health Center

Joint Audit & Compliance Committee Meeting
THIS PAGE INTENTIONALLY LEFT BLANK
### Status of Assignments

<table>
<thead>
<tr>
<th>Audit Project</th>
<th>UConn (UC) or UConn Health (UH)</th>
<th>Planning</th>
<th>Fieldwork</th>
<th>Pre-draft/Draft Reporting</th>
<th>Final Draft/Final Report Issued</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty Consulting FY2018</td>
<td>UC/UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hartford Campus Relocation – 4th and Final Report</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Selected Contract - Gilbane Long Term Contract</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Cogeneration Power Plant Cybersecurity</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>John Dempsey Hospital Controlled Substance Monitoring</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Offsite Sports Venue Contracts</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Wireless Network Administration and Security</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Travel</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Energy Services Performance Contract Project – Phase 1 Report 2</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Student Clinical Placements</td>
<td>UC/UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Entrepreneurial Academic Programs</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Undergraduate Student Safety Training</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Selected Contract Review - CSI</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Patients Accounts Receivable and Contractual Allowance</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>On Call Contract Program</td>
<td>UC</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>ADA</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Wireless Network Administration and Security</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>John Dempsey Hospital Operating Room</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Research Data Security</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>TOTAL AUDITS (20)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(04) (08) (01) (07)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Special Projects/Consulting</th>
<th>UConn (UC) or UConn Health (UH)</th>
<th>Planning</th>
<th>Field Work</th>
<th>Review Pre-draft</th>
<th>Project Final</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respiratory Therapy</td>
<td>UH</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Procurement</td>
<td>UC</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilities Operations</td>
<td>UC</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Travel</td>
<td>UH</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL SPECIAL PROJECTS/CONSULTING (04)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(00) (04) (00) (00)</td>
</tr>
</tbody>
</table>
Management Actions Submitted to AMAS for Review
UConn and UConn Health

UC Athletics
UC Waterbury Campus
Aging of Overdue Management Actions by Functional Area
Based on Original Due Date
UConn

# of Overdue Management Actions

0 2 4 6 8 10 12 14 16 18 20

Functional Area

UC Athletics
UC Center for Students with Disabilities
UC EVP of Administration and CFO
UC Controller
UC Dining Services
UC General Counsel
UC Human Resources
UC Information Technology Services
UC School of Law
UC Logistics Administration
UC Office of Institutional Equity
UC OVPR
UC Procurement
UC Office of the Provost
UC Procurement
UC Public Safety
UC School of Engineering
UC Sponsored Program Services
UC Student Affairs Administration
UC Waterbury Campus
UC Labor Relations

> 1 year late 6-12 months late 3-6 months late 0-3 months late
Open Overdue Management Actions by Audit - Based on Original Due Date

UConn
Open Management Actions by Finding Category
UConn Health

Finding Category

- Business Process Improvement: 39
- Business Purpose: 1
- Documentation: 13
- Governance: 1
- Management Oversight: 5
- Monitoring: 5
- Physical Security of Assets: 1
- Policy: 6
- Regulatory Compliance: 19
- Segregation of Duties: 3
- Technology: 10
- Training: 2
- Use of Resources: 5

# of Open Management Actions
Open Overdue Management Actions by Risk Level
UConn and UConn Health

Risk Level:
- Low: 110 actions
- Medium: 97 actions
- High: 6 actions
High Risk Overdue Management Actions by Functional Area
UConn and UConn Health
Low

Meaningful reportable issue for client consideration that in the Auditor’s judgment should be communicated in writing. The finding results in minimal exposure to UConn or UConn Health and has little or no impact on the UConn’s or UConn Health’s compliance with laws and regulations. The issues related to this control weakness will typically not lead to a material error.

Medium

Significant exposure to the area under review within the scope of the audit. The finding results in the potential violation of laws and regulations and should be addressed as a priority to ensure compliance with UConn’s or UConn Health’s policies and procedures. The significance of the potential errors related to this control weakness makes it important to correct.

High

Significant exposure to UConn or UConn Health that could include systemic UConn or UConn Health wide exposure. The finding could result in a significant violation of laws and regulations and should be viewed as a highest priority which UConn or UConn Health must address immediately.
University of Connecticut
&
University of Connecticut Health Center

Joint Audit & Compliance Committee Meeting
UConn and UConn Health are committed to supporting our innovative faculty, students, and staff to promote global exchange and collaboration. The Office of the Vice President for Research (OVPR) is an important resource in helping the UConn community implement and adhere to the broad range of rules and regulations related to the conduct of sponsored research.

In this Compliance Chatter, the OVPR would like to remind the University community of the following:

**RESEARCH SUPPORT**

Be thorough and complete in disclosing and accounting for all forms of research support, whether or not that funding is passed through UConn or UConn Health.

Forms of research support include financial support and resources from sponsors, other institutions, and foreign entities (e.g., active and pending support included in grant applications and prior to award issuance). [See the OVPR website for Active and Pending Support](https://compliance.uconn.edu).
FOREIGN COMPONENTS

Remember, foreign components of federally funded research must be disclosed and approved in advance by the sponsor.

Click here for the NIH definition of “foreign component”.

SFI's / REMUNERATION

Significant financial interests such as equity in a publicly or non-publicly traded entity, salary support outside of UConn / UConn Health, or any remuneration such as income from consulting, honoraria, or paid authorships must be disclosed annually and may require prior approval.

EXTRAMURAL ACTIVITIES

Extramural professional activities, whether compensated or uncompensated, should be disclosed through the consulting approval process to determine if there are potential conflicts of interest or commitment.

RELATED RESOURCES

Visit the OVPR Website
View the Faculty Consulting Policy

UCONN POLICY

View the UCONN Policy on Financial Conflicts of Interest in Research

UCONN HEALTH POLICY

View the UCONN HEALTH Policy on Individual Financial Conflicts of Interest in Research

About Us | Join Our Listserv | Contact Us | View Other Editions
Did you know that employment authorization to allow international students to work in the U.S. is regulated by law? International students on F-1 and J-1 visas may only work on or off campus within the employment rules authorized by their visa.

**On Campus Work**

International students with F-1 visas may work on campus up to 20 hours per week during the academic term.

During a student's vacation term, international students may work more than 20 hours per week. However, international students graduating in summer or in a program requiring summer enrollment, are not considered to be in a vacation term and must restrict on campus employment to 20 hours per week.

**Please Note:** J-1 visa holders must obtain written authorization from UConn's International Student & Scholar Services (ISSS) prior to working on campus.

*Students who work on-campus more than 20 hours per week during the academic term, or who work off-campus without authorization may be in violation of their visa status.*
Off Campus Work

International students may not work off campus in any capacity without special authorization, including:

- An Employment Authorization Document permitting work for students with unexpected economic hardship

- A job or internship authorized by ISSS and U.S. Citizenship and Immigration Services for Optional Practical Training (OPT). OPT is for work directly related to the field of study and may be granted during and after a student’s academic program.

- An internship authorized by ISSS for Curricular Practical Training (CPT). CPT is for work that is part of the student’s academic curriculum, e.g. an internship that meets a course requirement or degree requirement.

Related Resources

- ISSS Website
- CPT Information
- OPT Information

Other Situations Requiring OPT or CPT Authorization

- Unpaid internships, clinical placements and practicum courses.

- When starting a business or participating in UConn entrepreneurial programs.
U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

Guidance Document
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:
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
U.S. Department of Justice
Criminal Division
Evaluation of Corporate Compliance Programs
(Updated April 2019)

“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?
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 9-47.120 FCPA Corporate Enforcement Policy, available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.

• 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).


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).
Healthcare Business Continuity Management and Disaster Recovery—No Longer an Afterthought in Today's World
Table of Contents

Increasing Threats in an Already Dynamic Environment 2
Elements of a Business Continuity Management Program 3
When Disaster Strikes: Defining Risk Areas 5
Strategies for Successful Business Continuity Management 9
Making Business Continuity Management an Organizational Priority 11
Conclusion: Internal Audit’s Vital Role 12
Increasing Threats in an Already Dynamic Environment

A healthcare organization's operations and network can be greatly impacted, or even shut down, due to a natural disaster or the harmful actions of bad actors.

The mass shooting in a Chicago hospital in November 2018 was a stark reminder that today's hospitals and health systems face an increasing array of dangers that threaten to disrupt patient care and business operations. Workplace violence in the healthcare industry overall is on the rise, with one recent U.S. Government Accountability Office study reporting healthcare workers at inpatient facilities are five to 12 times more likely to encounter nonfatal violence in the workplace than workers in other industries. Cyberattacks, which can bring down electronic health record (EHR) applications and other vital systems in a matter of seconds, also have become more commonplace.

And, of course, the threat of natural disasters, including hurricanes and fires, is ever present and seems to be increasing, especially in geographically vulnerable areas. A hospital in Paradise, California, may not reopen after sustaining significant damage in the November 2018 Camp Fire. And the effects of 2017’s Hurricane Harvey are still very much on the minds of hospital and healthcare facility management in the Houston region as they digest lessons learned and rebuild.

When disaster strikes in an industry as complex as healthcare, the effects can be far-reaching. The consequences of IT failures within a healthcare facility in today’s increasingly electronic, data-reliant environment are great, and clinical, operational and financial areas all are at risk should critical systems go down.

With patient lives on the line, the stakes are even higher in healthcare than in other, less complex industries. If hospitals cannot operate their many departments and cannot keep vital IT systems up and running, these organizations could be rendered unable to take care of patients who entrust their lives to them.

All healthcare organizations know the importance of having emergency response plans in place to immediately address disasters, whether natural or man-made. Furthermore, hospitals are required to follow Centers for Medicare & Medicaid Services (CMS), Joint Commission and state authority regulations for emergency preparedness. A primary component of an organization's disaster response is its ability to continue operations as the organization works to recover from a disaster. Business continuity management (BCM) accomplishes this by pre-emptively identifying and establishing plans to continue managing key business functions, processes and their associated IT- or non-IT-related dependencies to minimize the impact of unexpected events on the organization while trying to maintain seamless, uninterrupted operations.

Healthcare internal auditors can bring value to organizational leadership and governance by performing periodic reviews of the organization's BCM and disaster recovery (DR) planning objectives and strategies.
Elements of a Business Continuity Management Program

A well-thought-out BCM program allows an organization to continue functioning during a disaster and, ultimately, to fully recover normal business operations in a timely manner afterward. Through the process of business continuity planning, an organization identifies its main risks, processes and IT systems, and it then creates plans for remediation should a disaster occur.

Though they may intersect with emergency management plans, which are concerned with keeping patients and staff safe from harm during a disaster, business continuity plans (BCPs) are focused on continuing operations when main systems are down. Central elements of a BCM program include:

Business Impact Analysis

A business impact analysis (BIA) is a process to predict the impact on business processes and systems in the event of a disaster in order to develop strategies to recover. Conducting a BIA helps an organization prioritize recovery of each business process and define what those processes need from the following three perspectives:

• **People:** What are the minimum personnel requirements needed to conduct the business process?

• **Technology:** What IT resources (for example, software applications or systems) are required and considered critical to execute that business process?

• **Process:** What non-IT tools, such as patient care instruments and paper charting, are needed to support the process?

To conduct a BIA, business leaders seek input from department owners and stakeholders across the organization to help define and prioritize all critical business functions. A standardized process for establishing ownership and conducting a BIA should exist.

When drafting a BIA, the team doing so should use existing organizational documents and information, including results of the organization’s hazard and vulnerability analysis. Other input used for BIA development includes questionnaires (using a standard form) or interviews with experienced staff members within the various departments. Examples of questions to be addressed during a BIA include:

• What are the significant business processes in this department?

• What applications or systems are considered mission critical?

• What resources, including human resources (key players), are required for these business processes to function normally?

• What are the main financial and operational impacts to the department and organization if these business processes cannot be performed?

• What is the recovery time objective for each function? In other words, how long can the department function without doing this business process before it significantly affects the organization? (Number of hours? Days? Weeks?)

• How quickly can these processes be resumed should a downtime event occur?

• What are the department’s key dependencies? For example, is there another system that this department’s system interfaces with that also should be considered critical?

• Does the department or business unit produce information that is important to another unit? What would the impact be to that department if there is an outage?

• What resources, including personnel, would be required to recover from a major disaster or system outage?
Output from the BIA should show how important each business process is to supporting the organization overall and help the organization prioritize where it should focus its time, attention and resources in the critical period following a disaster. The input from each business unit is essential to provide a road map for IT in terms of which systems need to be brought back up in what time frame. It’s important to note that while the IT function ultimately is responsible for bringing technological systems back up, the business units or departments themselves should own the process of identifying critical systems.

**Business Continuity Planning**

Using the framework created during the BIA, organizational leadership then can move into creating a BCP. A BCP is a strategic plan that positions an organization’s high-risk business processes to be able to function should a disaster occur and major systems shut down.

To develop a business continuity plan, organizational leadership and members of the business continuity team or committee should meet with the crucial process owners within each department to create a plan that can be put into place should a catastrophic event occur. The plan should focus on how each department can minimize impact to the organization and continue operating at an acceptable level during an event. The more thorough the plan, the better (see “Strategies for Successful Business Continuity Management”). The plan should be clear enough for any person to follow, regardless of the individual’s everyday role or background.

**Disaster Recovery**

As a result of conducting a BIA and developing a BCP, the organization should now have a comprehensive list of applications and systems needed to continue operations and a prioritization plan for how quickly the IT department needs to be able to recover those applications and systems. This is known as a disaster recovery plan. While business continuity plans focus primarily on operations, disaster recovery plans largely are an IT endeavor to support operations. When developing DR plans, operational leadership should be involved so the IT department can understand operational processes that need to immediately continue in addition to the supporting applications. As with BCPs, DR plans should be thorough.

**Testing**

Another crucial component of a BCM program is testing of both business continuity and disaster recovery plans. Teams should conduct tests at least annually using either a tabletop simulation or a full-scale drill. Periodic testing of the plans helps expose incomplete and ineffective procedures that need to be revised or updated to strengthen and refine recovery plans.
When critical systems are severely damaged during a disaster, the negative effects on a healthcare organization are multipronged. While different types of disasters—extreme weather incidents, terrorist attacks, ransomware or smaller-scale incidents such as a software malfunction—produce different effects, consideration of risk areas is vital to making sure the organization is prepared to continue operating when crucial systems are down.

Following are examples of some of the biggest risks for healthcare organizations in clinical, operational, finance and IT areas as well as strategies for adequately preparing to continue operations should a disaster occur. The examples can help internal auditors review organizational BCM and DR preparedness and assess the effectiveness of existing plans.

**Clinical Risk Areas**

**Risk:**

*Clinicians cannot access the EHR and therefore cannot quickly or efficiently treat or diagnose patients. In addition, patients are unable to access their own health information or schedule or change appointments via patient portals.*

**Risk Prevention Strategies:**

- Have a redundant system in place so clinicians can access patient medical history and check for medication allergies; make sure downtime viewers are available for critical applications.

- Have a redundant system or backup (manual) patient portal system in place for patients to access their own medical information or to schedule or amend appointments.

- Develop manual processes for handing off patient information, such as lab information and patient orders, to the lab, the radiology department or other members of the care team.

- Involve medical professionals in BIA and BCP development exercises to make sure critical clinical equipment is prioritized and accounted for; clinicians can provide valuable input to IT about complicated, specialized equipment.
Risk:
Clinicians cannot access electronic systems and must transition to a manual, paper-based system, but newer, less-experienced clinicians are not familiar with how to document or work on paper.

Risk Prevention Strategies:
• Include staff training on paper-based charting in business continuity and DR plans.
• Make paper-based charts and forms readily available throughout the facility and easy to locate.
• Coordinate clinical training (charting) with laboratory staff to cover comprehensive steps for how lab results will be returned and shared.
• Assign a staff member to make sure doctors and nurses are documenting information correctly.

Risk:
Patient handoffs—whether internal or external—are confusing and ineffective due to critical systems being down and communication among clinical departments or with other community healthcare organizations being hindered.

Risk Prevention Strategies:
• As part of overall BCM, have clinical staff conduct an evaluation and inventory of where patient handoffs are likely to occur.
• Include a manual process for documenting internal and external patient transfers in business continuity and DR plans (for example, to document moving patients from ambulatory to an acute care setting internally or externally).
• Designate a staff member to have complete responsibility for patient handoffs when systems are down.
• Make year-round efforts to improve overall coordination among clinical departments, particularly between ambulatory and acute care settings.
• Coordinate with local healthcare facilities and other community organizations to design processes for patient handoffs, and then conduct periodic assessments and tests of those plans.

Operations and Finance Risk Areas
Risk:
Major utilities (for example, electricity and water) are brought down during a disaster, or the facility is damaged and rendered completely unusable.

Risk Prevention Strategies:
• Have a well-equipped command center in place with functioning utilities.
• Prearrange transportation to move patients and staff safely in the event of a disaster. Having learned from Hurricane Katrina, hospitals in the New York City area had arranged for ambulance companies to be on standby should patients need to be evacuated, and they were grateful for that foresight when Hurricane Sandy hit in 2012.5
• Schedule periodic inspections of facility backup generators.
• Plan for adequate amounts of fuel and other energy sources to sustain on-site operations in the event that patients and staff are restricted from transport.
• Have contingency plans in place for all major utilities.

Risk:
Critical patient care and facility supplies cannot be delivered or otherwise replenished, and patients cannot be transferred to another facility due to a building lockdown caused by severe weather, such as a blizzard, or other events, such as an earthquake.

Risk Prevention Strategies:
• As part of business continuity planning, staff should assess the organization’s inventory of critical supplies.
• Stock enough medicine, medical supplies, food, water, clean linens and other supplies to last for a predetermined amount of time; for many organizations, the goal is the Joint Commission’s Emergency Management 96-hour standard or compliance with guidelines from other local, state or federal authorities.
• For supplies typically ordered online, establish an alternative method for placing orders if systems are down.
• Have a plan in place to work with vendors to handle large orders that require advance payment before shipment (for example, orders of expensive pharmaceuticals) if online payments are not possible.

• With infection prevention a top priority, include plans for hiring a third-party service to continue cleaning linens and rooms if these services are not able to be performed in-house for a period of time.

• Have a plan in place for a third-party service to provide ongoing cleaning and sterilization of medical devices.

Risk:
The organization loses revenue because patients have to be turned away (diverted to another facility) because there is no backup (manual) system in place to intake patient health and billing information.

Risk Prevention Strategies:
• Have a process for manually collecting patient billing information, so financial services staff members have complete and correct billing information when they later submit claims.

• Implement a formal manual backup process for physicians to transcribe their notes if the patient accounting system (PAS) is down.

• Consider assigning a staff member sole responsibility to make sure physician notes are properly transcribed and are later captured in the PAS once it is back online.

IT Risk Areas
Risk:
The organization cannot recover vital systems and suffers negative impacts to patient care, reputational damage and financial losses, and it is in breach of federal, local and state regulatory requirements and potentially subject to fines.

Risk Prevention Strategies:
• Have a backup facility in place that is able to bring up the organization’s main servers and provide synchronous replication, redundancy and high availability.

• Keep backup copies of software, systems and files in an off-site or alternative location, and make sure they can be brought back up in a timely matter.

• Have redundancies in place on the network between multiple data sites. This gives the organization the ability to use another data site without disruption if one data site goes down.

• Establish contracts for redundant critical technologies such as a redundant internet connection.

• Make sure network capacity is adequate to move large data files between systems if necessary.

• Have an appropriate backup plan or disaster recovery plan for the organization’s interface engine (the open link or application that allows other applications within the network to communicate with one another).

• As part of the disaster recovery plan, note whether the organization is able to restore an earlier version of all critical systems.

• When considering backup capabilities and restoration timings, account for changes in complexity and volume of data over time (for example, a considerable increase in the number of patients since the last time business continuity plans were reviewed), and test the ability to migrate large data files from the backup systems to the primary systems.

• If the organization’s main building is not accessible (such as during a hazardous materials incident or due to fire or weather-related damage), have controls in place to make sure there is sufficient (remote) network bandwidth and proper equipment to allow staff to work either from home or at a predetermined off-site facility.

• If the organization's main building is not accessible (such as during a hazardous materials incident or due to fire or weather-related damage), have controls in place to make sure there is sufficient (remote) network bandwidth and proper equipment to allow staff to work either from home or at a predetermined off-site facility.

Risk:
During downtime, security is reduced, leaving patient health information, payment card information and other sensitive information at risk of being compromised.

"Have a process for manually collecting patient billing information, so financial services staff members have complete and correct billing information when they later submit claims."
**Risk Prevention Strategies:**

- In the recovered environment, have in place security controls that are the same as or comparable to those in the original environment.

- As part of DR, include a plan for simultaneously recovering the security functions that go with critical systems. For example, if there is a specific firewall in place to protect sensitive patient records, the disaster recovery plan should include that firewall, and it should be brought back up with the EHR.

- Create a plan for destroying any confidential information that was captured on paper during downtime procedures, and decide as an organization how long the paper should be kept in case it needs to be referred to (for example, should the paper be scanned so there is an electronic copy?).

**Risk:**

*As healthcare organizations outsource more and more systems and processes, they are reliant on third parties to maintain critical applications and systems, whether stand-alone applications or those integrated with other in-house applications.*

**Risk Prevention Strategies:**

- Coordinate disaster recovery plans and business continuity plans with all vendors providing third-party applications or hosting critical applications.

- Share updates to BCPs and DR plans, and conduct periodic joint tests with vendors, depending on the criticality of the applications.
Strategies for Successful Business Continuity Management

The following are some of the areas healthcare organizations most commonly overlook when creating business continuity and disaster recovery plans as well as strategies for making those plans more effective.

**Revisit business continuity plans and DR plans often.** Business continuity and disaster recovery plans are not static documents meant to be created one time and then put away on a shelf. They should be revisited consistently and revised as needed based on changes to departmental processes and software or other infrastructure changes. Commonly overlooked in this area are changes to technology vendors or new IT systems that weren't reflected in the original BC and DR plans. A process should be in place to capture such changes. In addition, BCPs contain vital staff and vendor contact information. As this information changes frequently, plans should be reviewed periodically and updated when contact information changes such as when there is employee turnover. To capture staff information, consider sending an annual or biannual email to employees as a reminder to provide updated contact information to organizational leadership.

**Keep business continuity and disaster recovery plans in multiple formats.** Unfortunately, some organizations have learned the hard way the consequences of relying on only one format when paper-only plans have burned during a fire or an electronic-only plan was rendered inaccessible due to a system crash or ransomware attack. Keeping BC and DR plans in multiple formats and storing backups off-site are essential practices.

**Don't overlook outlier or affiliated facilities.** Larger organizations need to consider and include in their BCPs and DR plans any external facilities, such as behavioral health clinics, imaging centers or other free-standing centers belonging to the health system or existing as part of a joint venture with another health system.

**Seek input from local authorities and community partners.** Working with local community leaders and authorities such as police, fire departments and other healthcare providers is critical when creating BC and DR plans. Local partners can be called on for assistance with emergency response, transportation and even patient care during a disaster affecting the individual facility or one that is widespread throughout a region.

**Clearly define roles.** Plans should detail who has the authority to declare a disaster and define roles for the organization's disaster recovery team. Depending on the size of the entity, four or five people typically make up the overall disaster recovery team, covering areas such as communications and media relations, resources and supplies and workforce. Each of these people will lead a team of individuals who can take action during an event and make sure disaster recovery and business continuity plans are executed. The IT department typically has a separate disaster recovery team that includes a point person who determines budget and resource allocation and maintains contact with vendors.

**Identify in advance any temporary staffing or vendors that might be needed during a disaster.** Business continuity plans should include contact information for additional staff required. Consider assigning a staff member the role of managing temporary staff during a downtime or disaster event.

**Keep up with training.** Training staff in BCM and disaster recovery may seem like one more to-do item in an increasingly busy work environment; however, in the midst of a disaster is not the time to learn about the organization's business continuity and disaster recovery plans. Organizational leadership should require training at regular intervals—at least annually—and be sure to include plans for training new employees during the onboarding process.

**Consider having a third-party consultant review the organization's plans.** An outside perspective can help organizational leadership challenge existing business continuity and disaster recovery plans and note areas for improvement. The bird's-eye view can be valuable, especially for organizations that have been experiencing change in management, operations or IT systems and for those that have been using similar plans for many years.
Test, test and test some more. Testing the overall business continuity plan, including disaster recovery, is paramount to validating effectiveness in the event of a disaster. Testing should be conducted at least annually, and many organizations benefit from more frequent testing, depending on the size and scope of the facilities involved. Some organizations find tabletop exercises to be helpful. During these events, key stakeholders from departments across the organization walk through various disaster scenarios featuring loss of IT systems. These tabletop exercises typically include “injects” in which twists to the scenario are added to help participants probe what they might do should scenario X, Y or Z happen.

Some organizations’ IT departments periodically conduct downtime exercises during which they take down a main system, such as the organization’s EHR, and then try to restore it from backup within a specified time frame. And many organizations already practice full-scale disaster simulation drills, such as those required by CMS.6

Finally, whether conducting a full-scale, communitywide drill or a biweekly IT downtime simulation, organizations should have a formal procedure to capture and address lessons learned from tests performed. Also, lessons learned from other organizations that could experience the same or even different types of disasters should be evaluated, wherever possible, so additional perspectives can be considered. This will help organizations be even better prepared for various disaster scenarios. Just as facilities learn valuable lessons after the fact when an actual event occurs, indispensable insights can be gleaned from drills and other simulation exercises, with the information then being used to revise and update BC and DR plans.
Making Business Continuity Management an Organizational Priority

For business continuity management efforts to be most successful, they need to be among an organization’s top priorities. This can be an understandably tall order for many healthcare organizations in an era marked by stretched financial and human resources.

As with many organization-wide initiatives, business continuity management requires a commitment of support from organizational leadership, including the board. The following strategies for making business continuity management more of an organizational priority should be considered:

• Include discussion about BCM on the board’s and C-suite’s meeting agendas. Help establish or enhance tone at the top.

• Appoint a member of the leadership team to own business continuity management, including responsibility for updating plans at least annually; depending on organizational size, this may be the individual’s sole job.

• Include discussion about BCM and DR plans in daily or weekly departmental meetings.

• Regularly communicate information about BC or DR plans with staff members to increase awareness.

• Consider the impact to BC and DR plans when implementing new IT systems, moving applications to a hosted environment or making significant changes to operating departments.

• Consider including a BCM-related objective on senior leaders’ annual reviews.

“As with many organization-wide initiatives, business continuity management requires a commitment of support from organizational leadership, including the board.
Conclusion: Internal Audit’s Vital Role

In a complex and continuously evolving healthcare industry that faces more threats than even just a decade ago, today’s hospitals and health systems need to be more prepared than ever to continue operations should a disaster occur. Healthcare internal auditors play a critical role in assessing whether an organization is meeting business continuity management objectives. These objectives include formulating thorough, standardized business continuity and disaster recovery plans—with considerations for the essential processes, personnel and resources, including external partners, needed to navigate an event—and overseeing testing and follow-up for all plans.

Working with organizational senior leadership, healthcare internal auditors can help make sure business continuity management is effective so the organization is ready to serve patients even when unexpected events occur, disasters strike or major systems are unavailable.

Endnotes:


ABOUT AHIA

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge, and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network, www.ahia.org. AHIA white papers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. By providing healthcare specific information and education, white papers can help practitioners evaluate risks, develop priorities, and design audit approaches. It is meant to help readers understand an issue, solve a problem, or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content clearly related to healthcare internal auditing that does not promote commercial products or services. Interested? Contact a member of the AHIA White Paper Subcommittee.

SUBCOMMITTEE:

Alan Henton, White Paper Chair
alan.p.henton@vumc.org

Debi Weatherford
debi.weatherford@piedmont.org

Mark Eddy
mark.eddy@hcahealthcare.com

Laura L. Sak-Castellano
Laura.Sak-Castellano@advocatehealth.com

Linda Greer
tlbmc@cox.net

Deborah Pazourek, AHIA Board Liaison
Deborah.L.Pazourek@medstar.net