**IOWA BOARD OF REGENTS AUDIT AND COMPLIANCE COMMITTEE APPENDIX**
**APRIL 22-23, 2026**

**Contact: Chad Sharp**

## INTERNAL AUDIT REPORTS ISSUED

| ORIGINAL REPORTS | CEA* | Status |
|---|---|---|
| **University of Iowa** | | |
| • Bioengineering |  | Open |
| • Medical Center University Patient and Visitor Parking |  | Open |
| • North Liberty Building Hospital Access and Security |  | Open |
| • Red Card Administration |  | Open |
| • Research Integrity and Security Office |  | Open |
| • Women's Resource Action Center |  | Open |
| **University of Northern Iowa** | | Open |
| • UNI Works |  | Open |

| | |
|---|---|
| **HIGH**  | • Could seriously affect several areas within the university. Exposes the university to unacceptable risks or liability if not corrected OR<br>• Involves difficult issues requiring the attention of executive management OR<br>• Involves compliance with Federal, State, or other laws and could result in serious consequences if not implemented OR<br>• Unacceptable weakness in the internal and/or accounting controls OR<br>• Substantial savings (perhaps millions) can potentially be realized by correcting. |
| **MODERATE**  | • Could seriously affect a department or area within the university OR<br>• Involves a difficult issue requiring the attention of upper management OR<br>• Involves compliance with Federal, State, or other law and could result in minor consequences if not implemented OR<br>• Weakness in the internal and/or accounting controls OR<br>• Savings (perhaps thousands) can potentially be realized by correcting. |
| **LOW**  | • Can affect a department or may be common to several areas OR<br>• Could result in improved internal and accounting control OR<br>• Can be corrected relatively easily OR<br>• Could result in improved efficiency or effectiveness of operations OR<br>• No reportable observations or corrective action taken prior to report issuance. |

**The internal auditors have utilized the colors for the CEA in evaluating each overall audit report.*

## INTERNAL AUDIT REPORTS ISSUED

**University of Iowa**
**Bioengineering**
*Issued April 22, 2026* Status: Open

Bioengineering is responsible for the maintenance of patient medical equipment at the Medical Center University, Medical Center North Liberty, Iowa River Landing, Medical Center Downtown, and off-site clinics throughout Iowa. The Bioengineering audit was performed to evaluate if proper controls are in place and determine whether opportunities for improvement exist. Audit recommendations include regularly monitoring equipment records for accuracy of preventative maintenance status, implementing more frequent inventory counts, developing and monitoring key performance metrics, performing regular billing reviews, identifying additional vehicle resources to support departmental operations, involving additional staff in the rate-setting process, and establishing a process to monitor third party contractor operations. Management expects to complete its action plans by September 2026.

**University of Iowa**
**Medical Center University Patient and Visitor Parking**
*Issued April 22, 2026* Status: Open

University of Iowa (UI) Health Care Medical Center University (MCU) campus' patient and visitor parking facilities are operated by UI Parking and Transportation (P&T). P&T invoices UI Health Care monthly for patient parking passes. MCU patient and visitor parking service terms are outlined in a Memorandum of Understanding (MOU) between UI Heath Care and P&T. The audit was performed to evaluate if proper controls are in place and determine whether opportunities for improvement exist. Primary recommendations include establishing multi-disciplinary oversight of patient and visitor parking policies and standards; updating communication plans for program message distribution; developing training programs; and updating processes in support of MCU parking strategies, MOU terms, and parking needs for patients and visitors. Additional recommendations include submitting a formal project request to review viable system integration options and implementing a mutually agreed-upon parking solution. Management expects to complete its action plans by January 2027.

**University of Iowa**
**North Liberty Hospital Building Access and Security**
*Issued April 22, 2026* Status: Open

The UI Health Care Medical Center North Liberty Department of Safety and Security oversees building access control and security processes for the North Liberty hospital. The audit evaluated if proper access and security controls are in place and determine whether opportunities for improvement exist. Primary audit recommendations include increasing vendor representative building access controls, implementing regular badge access and security systems reviews, and improving key tracking system controls. Management expects to complete their action plans by May 2026.

**University of Iowa**
**Red Card Administration**
*Issued April 22, 2026* Status: Open

Red Card is a software application utilized by Athletics to provide meal funding to student athletes allowing them to purchase meals and grocery items in the Iowa City area. The audit was performed to evaluate if proper controls are in place and determine whether opportunities for improvement exist. Audit recommendations include improving Red Card user access and team roster management and establishing a process for improved oversight of prohibited item purchases. Management expects to complete its action plans by April 2026.

**University of Iowa**
**Research Integrity and Security Office**
*Issued April 22, 2026* Status: Open

The Research Integrity and Security Office, within the Office of the Vice President for Research, supports the research enterprise at the University of Iowa by promoting ethical, secure, and compliant research practices. The audit was performed to evaluate if proper controls are in place and determine whether opportunities for improvement exist. Audit recommendations include implementing and documenting internal change management procedures for federal agency requirements and formalizing the review process for international travel training materials.

**University of Iowa**
**Women's Resource and Action Center**
*Issued April 22, 2026* Status: Open

The Women's Resource and Action Center (WRAC) is a non-revenue producing department within the Division of Student Life that administers several programs including Iowa National Education for Women (N.E.W) Leadership, Weaving our Community Network, and Night Slice. WRAC also offers violence prevention training, space reservation, and counseling services to University of Iowa faculty, staff, students and the surrounding community. This audit was performed to evaluate if proper controls are in place and determine whether opportunities for improvement exist. Primary audit recommendations include implementing processes to review physical and system access, creating a new general ledger account for restricted gift funds, working with Purchasing for proper approval of a memorandum of understanding, and monitoring trainings for proper assignment and completion. Management expects to complete its action plans by July 2026.

**University of Northern Iowa**
**UNI Works**
*Issued April 22, 2026* Status: Open

The University of Northern Iowa (UNI) implemented UNI Works in July 2024, which is a cloud-based enterprise resource planning software application powered by Workday. The audit assessed the efficiency and effectiveness of the Workday system, including governance, processes, controls, and training, to determine whether it supports consistent operations, effective oversight, and system optimization. Primary audit recommendations focused on establishment and implementation of the UNI Works governance structure; audit logging and monitoring expectations; creation of a business continuity and disaster recovery plan; prioritization of issue tracking; and license optimization processes. Management expects to complete its action plans by April 2027.

BOARD OF REGENTS
Governing Iowa's Public Universities

## Office of Internal Audit

IOWA

# Bioengineering

**April 22, 2026**

**Distribution List**
Barbara Wilson, President
Denise Jamieson, Vice President for Medical Affairs and Dean, Carver College of Medicine
Brad Haws, Chief Executive Officer, Clinical Enterprise, Associate Vice President, UI Health Care
Mark Henrichs, Associate Vice President for Finance and Chief Financial Officer, UI Health Care
Jody Reyes, Chief Operating Officer, Clinical Enterprise, UI Health Care
Mike Brownlee, Chief Administrative Officer, Medical Center University, UI Health Care
J. Joshua Wilda, Associate Vice President for Information Systems and Chief Information Digital Officer, UI Health Care
Mark Heston, Director, Bioengineering
Greg Larson, Assistant Director, Bioengineering
Jennifer Miller, Chief Administrative Officer, Medical Center Downtown, UI Health Care
Terry Johnson, University Chief Financial Officer and Treasurer
Iowa Board of Regents
Office of Auditor of State

# Bioengineering

**BACKGROUND**

Bioengineering is responsible for maintaining patient medical equipment at Medical Center University (MCU), Medical Center North Liberty (MCNL), Iowa River Landing (IRL), Medical Center Downtown (MCD), and off-site clinics throughout Iowa. The University of Iowa (UI) currently has a contract with a third-party vendor, Renovo, to provide bioengineering services to MCD through December 2026. Bioengineering's total revenue for fiscal year (FY) 2025 was $4.3 million, from sales and services to other university departments.

Bioengineering provides maintenance services for approximately 45,000 individual devices and pieces of equipment. Bioengineering employs 35 full-time staff and is comprised of 5 specialty teams. The inpatient team is responsible for equipment on patient floors; perioperative is responsible for operating rooms (OR), ambulatory surgery centers (ASC), and digestive health; ambulatory is responsible for internal and external clinics; the bed shop is responsible for patient beds and lifts; and the bench team is responsible for smaller equipment. In addition to Bioengineering, three other departments support equipment maintenance, including Health Care Information Systems (HCIS) for networking issues, Radiology Engineering for radiology equipment, and Engineering Services for physical repairs.

Bioengineering currently utilizes Cherwell for asset management, but system capabilities, including reporting, are limited as it was not designed for biomedical-asset tracking. The department is in the process of transitioning to a new asset management system, TMA. Bioengineering has one departmental vehicle, used primarily by the ambulatory team, to travel to off-site clinics to provide preventative maintenance (PM) and repair services.

**PURPOSE AND SCOPE**

The purpose of this audit was to provide reasonable assurance that controls are in place and operating as intended, and to determine whether opportunities for improvement exist. The audit objectives were to verify whether:

- Controls over parts inventory management processes are in place and effective.
- Required equipment maintenance is performed timely and in alignment with manufacturer guidelines.
- Controls are effective at ensuring that Bioengineering is involved in purchasing decisions for equipment that it is responsible for maintaining.
- Bioengineering processing of new equipment is consistently performed and aligns with university policies and procedures.
- Drivers are compliant with the University Driving Policy.
- Fees-for-service are established, applied consistently, and reviewed on a regular basis.
- Controls over the billing cycle are in place and effective.

The audit scope included procedures, controls, and related transactions from FY 2025 to the present. On-site audit observations were conducted at Bioengineering MCU and MCD. There were no reportable findings related to equipment purchasing, new equipment processing and driver compliance.

**DISCUSSION AND AUDIT RECOMMENDATIONS**

**1) Equipment – PM**

*Discussion* – Device PM statuses on the Bioengineering PM report are not consistently updated, increasing the risk of delayed or missed equipment PM. Additionally, devices that do not require regular maintenance are not differentiated from those that do, resulting in unclear PM records. Bioengineering relies on Cherwell to automatically update the PM status and next PM date for devices once PM is completed. This automatic status update is not always occurring as intended. Out of 15 tested devices on the PM Schedule Report, there were 3 overdue; one device is no longer active, one device is used for training purposes, and one device is being removed from service and has only been tracked in the PM report for inventory purposes. Bioengineering technicians receive a PM due list from Cherwell to work from and can correct statuses in the system as needed but management does not regularly monitor the statuses to verify accuracy. System reporting capabilities are limited in tracking inactive devices, training devices, and devices not used in patient care. While system reports and records do not consistently represent accurate PM statuses, all PM inspection requirements are properly aligned with manufacturer PM schedules.

*Audit Recommendation* – Management should update the PM status for equipment records with inaccurate statuses and perform regular reviews to verify that records are automatically updated as intended. Management should consider flagging equipment that is on the PM Schedule Report but is not used in patient care or separately tracking this equipment that does not require regular maintenance.

*Management's Action Plan* – Management will implement a process to verify records are accurately updated after PM occurs to verify the system is operating as intended and will update the PM status for equipment records with inaccurate statuses. Management will note or track equipment that is on the PM list but is not used in patient care and does not require regular maintenance. Monitoring may be reduced or removed as trust is gained in the system.

*Individuals Responsible* – Director, Bioengineering and Assistant Director, Bioengineering

*Target Date* – July 2026

**2) Parts Inventory Management**

*Discussion* – Bioengineering is not regularly reviewing unfulfilled incident reports, increasing the risk of inaccurate inventory counts. Out of 15 items tested, 5 had inventory count discrepancies caused by system limitations and known errors that were in the process of being manually corrected. Identifying causes of count discrepancies requires manual review from the technician. While Bioengineering performs an annual full part inventory count during the year, there are limited controls in place to identify mid-year errors. Out of the five items with inventory count discrepancies, two discrepancies were due to not being reconciled and updated in Cherwell at the time the inventory count was performed, one was due to not being charged to a work order or was counted incorrectly during the most recent inventory count, and two were due to special-order category limitations within the system.

*Audit Recommendation* – Management should implement more frequent inventory counts and monitor unfulfilled incident reports on a regular basis to correct inventory record errors promptly.

*Management's Action Plan* – Management will implement more frequent-cycle inventory counts that will count the highest-value parts every 30 days, the next-most-valuable parts every 60 days, and the lower-value parts every 90 days.

*Individuals Responsible* – Director, Bioengineering and Assistant Director, Bioengineering

*Target Date* – September 2026

**3) Key Performance Indicator (KPI) Reporting**
*Discussion* – Bioengineering has not developed or implemented KPIs due to system limitations, increasing the risk of inefficiencies and underperformance. The purpose of establishing KPIs is to identify areas of improvement, track and monitor operational goals and efficiencies, benchmark employee performances, and set clear employee performance expectations, allowing management to identify performance issues sooner and take appropriate action when required.

*Audit Recommendation* – Management should develop KPIs and department-wide quality metrics to set clear departmental performance expectations. Management should develop reports to monitor these metrics and manage any changes or significant trends.

*Management's Action Plan* – Bioengineering will establish KPIs and monitor them through TMA. Reporting KPIs will be monitored by leadership and presented to key stakeholders on a periodic basis.

*Individuals Responsible* – Director, Bioengineering and Assistant Director, Bioengineering

*Target Date* – September 2026

**4) Billing Reviews**
*Discussion* – Bioengineering does not have monitoring in place to perform billing accuracy reviews, increasing the risk of billing errors and missed billing. Higher level financial reviews are completed by the departmental director, but no specific review of billing is completed due to system reporting limitations. A charge accuracy review was performed on all October 2025 billing to verify the hourly rate charged with total amounts charged for each incident and no discrepancies were identified.

*Audit Recommendation* – Management should create a process to perform regular reviews to verify billing completeness and accuracy.

*Management's Action Plan* – Management will develop reports to support regular monitoring of billing completeness and accuracy. Monitoring will include verifying correct general ledger accounts are charged, time billed is reasonable, and charges are accurate.

*Individuals Responsible* – Director, Bioengineering and Assistant Director, Bioengineering

*Target Date* – August 2026

**5) Departmental Vehicle**
*Discussion* – Bioengineering only has one departmental vehicle for technicians to use to visit UI Health Care off-site locations, increasing the risk of delayed preventative maintenance and repairs and potentially impacting patient care. Vehicle scheduling is completed via email between the Bioengineering teams and scheduling conflicts can occur when off-site repair requests conflict with each other or with planned preventative maintenance. The vehicle is also unavailable while being maintained. While scheduling conflicts are uncommon, conflicts result in the delay of either repair or preventative maintenance. One such conflict resulted in delaying the repair of a patient bed at an off-site clinic for

more than a week due to no back-up vehicle being available, resulting in a patient bed being out of service during that time.

*Audit Recommendation* – Management should work with UI Community Clinic's administration and Parking and Transportation to identify whether existing resources can be used to support Bioengineering's off-site repair and maintenance responsibilities.

*Management's Action Plan* – Management will work with Fleet Services and off-site locations to determine if there are any existing vehicle options available and will evaluate if Bioengineering needs a second vehicle. Management will work with the ambulatory team to determine the best way to schedule use of the vehicle(s).

*Individuals Responsible* – Director, Bioengineering and Assistant Director, Bioengineering

*Target Date* – September 2026

**6) Rate-Setting Process**

*Discussion* – The Bioengineering rate-setting process is solely performed by the Bioengineering Director without secondary approval or review and processes are not formally documented, resulting in the increased risk of inconsistent rate-setting practices and inefficiency during personnel changes. The UI Service Center Policy states, *"Service center rates should be set so the center breaks even…up to a 10% (positive or negative) fund balance, as a percent of current year expenditures, will be considered acceptable by university standards."* Financial Operations does not monitor Bioengineering's rate-setting process and HCIS only monitors it to ensure the department's end-of-year fund balance is within a break-even threshold of plus or minus 10% of current-year expenditures. Bioengineering has planned to train one of the assistant directors on this process, however, this has not occurred yet and access to this documentation has not been granted.

*Audit Recommendation* – Management should formally document the rate-setting process and train additional staff on the rate-setting process. Annual rate-setting calculations should be reviewed by a secondary person or party.

*Management's Action Plan* – Management will verify and document the rate-setting process. Rates will be reviewed annually, and accounting will be reviewed throughout the year by the Bioengineering director or assistant director to ensure the department's end-of-year fund balance is not exceeding the plus or minus 10% of current-year expenditures.

*Individuals Responsible* – Director, Bioengineering and Assistant Director, Bioengineering

*Target Date* – September 2026

**7) MCD Renovo Reporting Access**

*Discussion* – Bioengineering does not currently have access to reporting from Renovo, increasing the risk that equipment is not managed properly. Existing Renovo reports include a monthly dashboard of KPIs, current PM tasks, and lists of equipment overdue for PM by 30, 60, and 90-days. The contract with Renovo states, *"Renovo will provide client with records and reports necessary to monitor Services effectiveness. All required scheduled maintenance and repair documentation will be documented and recorded within RenovoLive, Renovo's computerized information management system, and will be accessible by client."* Bioengineering does not currently have access to the MCD equipment list or receive reporting from

Renovo as outlined in the contract. Renovo provides regular reporting to the Environment of Care Work Group whose purpose is to provide oversight for clinical operations at UI Health Care to ensure high quality patient care, safety and compliance with regulations. Currently, there is no additional monitoring of Renovo activities being performed by UI Health Care.

*Audit Recommendation* – Bioengineering should work with MCD administration and Renovo to establish a process to monitor Renovo activities.

*Management's Action Plan* – Management will work with Renovo leadership to determine the best process to receive and monitor monthly reporting.

*Individuals Responsible* – Director, Bioengineering and Assistant Director, Bioengineering

*Target Date* – May 2026

**SUMMARY**

Management has been responsive to the recommendations made during the audit. The successful implementation of the audit recommendations will further strengthen the Bioengineering control environment. Internal Audit will initiate a follow-up in the first quarter of FY 2027 to verify corrective actions have been implemented.

Bonnie Carter, Auditor

James Pitcher, Assistant Audit Director

Chad Sharp, Chief Audit Executive

BOARD OF REGENTS
Governing Iowa's Public Universities

## Office of Internal Audit

IOWA

# Medical Center University Patient and Visitor Parking

**April 22, 2026**

**Distribution List**
Barbara Wilson, President
Denise Jamieson, Vice President for Medical Affairs and Dean, Carver College of Medicine
Brad Haws, Chief Executive Officer, Clinical Enterprise, Associate Vice President, UI Health Care
Jody Reyes, Chief Operating Officer, Clinical Enterprise, UI Health Care
Katie McKinnon, Administrative Chief of Staff, Clinical Enterprise, UI Health Care
Mark Henrichs, Associate Vice President for Finance and Chief Financial Officer, UI Health Care
J. Joshua Wilda, Associate Vice President for Information Systems and Chief Information Digital Officer, UI Health Care
Debby Zumbach, Associate Vice President and Director, Business Services and Parking and Transportation
Kyle Anson, Associate Vice President, Human Resources, UI Health Care
Nicholas Dreyer, Executive IT Director, Health Care Information Systems
Lisa Brewster, Senior Director, Human Resource Services, UI Health Care
Jeff Rahn, Management Services Assistant Director, Parking and Transportation
Terry Johnson, University Chief Financial Officer and Treasurer
Iowa Board of Regents
Office of Auditor of State

# Medical Center University Patient and Visitor Parking

**BACKGROUND**

University of Iowa (UI) Health Care Medical Center University (MCU) Campus' patient and visitor parking facilities, located at 200 Hawkins Drive, are operated by UI Parking and Transportation (P&T). P&T is a self-supporting unit providing parking for the university. P&T invoices UI Health Care monthly for patient parking passes. Hospital parking service terms are outlined within a Memorandum of Understanding (MOU), signed in October 2024, between UI Heath Care and P&T. The MOU includes operating logistics, parking facility management, operational improvement efforts, and parking validation at the MCU campus.

Multiple technology systems are used to support parking services including UI Health Care's medical record system, Epic, and UI P&T's parking system, Amono McGann. During fiscal year (FY) 2025, 623,800 parking passes were distributed at a total cost of $2.45 million, with 95% of the covered services representing patient parking passes funded by UI Health Care. The patient passes are single-use parking passes generated from Epic to pay for parking during the duration of a patient's healthcare appointment including outpatient visits, labs, surgeries, or procedures. The other parking pass types utilized are volunteer, clergy, grieving family and friends, visitor parking pass booklets, and service recovery passes to address delays or appointment rescheduling that result in prolonged parking for the patient.

**PURPOSE AND SCOPE**

The purpose of this audit was to provide reasonable assurance that controls are in place and operating as intended and to determine whether opportunities for improvement exist. The audit objectives were to verify:

- Operational and administrative controls for hospital parking are properly implemented to support university and UI Health Care strategic goals and institutional standards.
- Information technology (IT) and project management controls were implemented to ensure MOU requirements were properly captured and system changes were deployed in accordance with the institutional change management process.

The audit scope included current MCU procedures, controls, and related transactions from FY 2025 to the present. The Medical Center North Liberty and Medical Center Downtown parking facilities were not included in the scope of this audit as they are covered under separate agreements.

**DISCUSSION AND AUDIT RECOMMENDATIONS**

**1) Hospital Parking Oversight**

*Discussion* – There is no oversight structure in place to support UI Health Care MCU's parking strategies and MOU terms, increasing the risk that parking programs and practices will not achieve desired results. Through staff interviews, observations, and review of documented procedures and parking-related staff communication, it was identified that there is a lack of:

- Current parking communication plans and messaging for different audiences.
- Parking policies or standards specific to the hospital parking program.
- Assigned points of contact for parking-related responsibilities across MCU.
- Parking pass policy information provided to employees during onboarding and throughout employment.

- Regular MCU enterprise review and update of parking procedures, training, tools and presentations.
- Monitoring of MCU parking program effectiveness.
- Reporting from technology solutions used to perform automated reconciliations and investigations.
- Process to submit or identify other enhancements or efficiencies to improve the program.

The MOU states, *"this MOU, including Services and Compensation, will be reviewed annually to determine additional operational efficiencies and processes that may be limiting or negatively impacting the operating effectiveness of the agreement."* These deficiencies in the existing program environment have resulted in inconsistent processes and a limited understanding of existing systems and controls.

*Audit Recommendation* – UI Health Care should establish multi-disciplinary oversight for hospital parking with financial, operational, IT, and other appropriate management representation. An updated communication plan to provide multiple methods of distributing parking program messaging should be implemented. A process for development and review of training and compliance programs, that create and align with MCU enterprise hospital parking policies and standards, should be created. A cross-functional team should review and update operational processes to support MCU parking strategies, MOU terms, and parking needs for patients and visitors in consultation with UI P&T.

*Management's Action Plan* – Management will establish a multi-disciplinary oversight committee for patient and visitor parking to:

- Develop and maintain hospital specific parking guidelines related to patient and visitor parking, including evaluation of reconciliation and compliance monitoring processes.
- Develop and review staff and volunteer training and compliance programs for patient and visitor parking that create and align with enterprise hospital parking policies and standards.
- Create and maintain communication plans for patient and visitor parking education and messaging throughout the organization.
- Review and update processes and guidelines to support parking strategies, MOU terms, and parking needs for patients and visitors in consultation with UI P&T.
- Include operations, finance, human resources, marketing and communications, nursing, volunteer services, and IT representation.

*Individual Responsible* – Administrative Chief of Staff, Clinical Enterprise, UI Health Care

*Target Date* – July 2026

**2) Project Management**

*Discussion* – No formal project was developed to determine if IT integration is viable between the UI Health Care and UI P&T systems, resulting in challenges to adequately manage the current parking processes. The MOU covering parking service terms included evaluating viable options related to the integration of IT systems. The MOU states, *"UIHC and UI P&T agree that both Parties will work with their respective vendors to determine if IT integration between the respective platforms (Amano McGann and Epic at time of agreement) is a viable option. Amano McGann is agreeable to pursuing a unique QR code for each patient. This should be a priority for both parties to implement in FY25. Should this option not be viable, both Parties will continue to work toward a mutually agreed upon solution to ensure optimization of the patient parking voucher."* The MOU also states UI Health Care "*remains committed to evaluating*

*and developing options for smart and mobile technology to replace current printed vouchers, including volunteer and clergy validations."*

Upon approval of the MOU, UI Health Care leadership requested an initial review be performed by Health Care Information Systems (HCIS) to explore possible requirements for changes and enhancements to Epic, to better support hospital parking. However, no formal project was developed to review the options available as noted in the MOU. Additionally, there were no discussions with vendors to further explore technology solution options, including interface and system functionality available to support parking services.

*Audit Recommendation* – A formal project should be submitted through the standard HCIS process, allowing parties to review viable options for IT integration with Epic and Amano McGann systems, while exploring the use of unique patient-specific codes. Additionally, the project should include review of options for a mobile solution. If IT integration is not viable, both UI Health Care and UI P&T should work toward a mutual agreement on a solution to ensure optimization of the patient parking voucher.

*Management's Action Plan* – An executive review of the MOU and project intent will be performed to determine the supported written or revised agreement terms. Upon confirmation of the approved MOU requirements, a Project Initiation Document will be submitted to the HCIS Project Management Office. HCIS and UI P&T will coordinate with Epic and Amano McGann to evaluate whether technical integration between the two systems is feasible, including unique patient-specific identifiers and mobile options for a patient parking pass to replace or supplement printed vouchers. If full IT integration is determined to be non-viable, UI Health Care and UI P&T will collaboratively define and document alternative workflow and technology options to optimize the patient parking validation process. Once an agreed-upon solution is identified, implementation will be completed based on the overall complexity, scope, and resource requirements of the selected solution.

*Individuals Responsible* – Executive IT Director, Health Care Information Systems, and Management Services Assistant Director, Parking and Transportation

*Target Date* – January 2027

**SUMMARY**

Management has been responsive to the recommendations made during the audit. The successful implementation of the audit recommendations will further strengthen the control environment and increase the integrity and transparency of the parking program. Internal Audit will initiate a follow-up in the third quarter of FY 2027 to verify corrective actions have been implemented.

Julie Appleget, Senior IT Auditor

Kip Druecker, Audit Manager

James Pitcher, Assistant Audit Director

Chad Sharp, Chief Audit Executive

BOARD OF REGENTS
Governing Iowa's Public Universities

## Office of Internal Audit

IOWA

# North Liberty Hospital Building Access and Security

**April 22, 2026**

**Distribution List**
Barbara Wilson, President
Denise Jamieson, Vice President for Medical Affairs and Dean, Carver College of Medicine
Brad Haws, Chief Executive Officer, Clinical Enterprise, Associate Vice President, UI Health Care
Mark Henrichs, Associate Vice President for Finance and Chief Financial Officer, UI Health Care
Jody Reyes, Chief Operating Officer, Clinical Enterprise, UI Health Care
Amy O'Deen, Chief Administrative Officer, Medical Center North Liberty, UI Health Care
Bryan Garter, Director of Operations, Medical Center North Liberty, UI Health Care
Robert Kwiat, Director, Safety and Security, Medical Center University, UI Health Care
Frank Eischens, Director, Supply Chain, UI Health Care
Dustin Wherry, Senior Supervisor, Safety and Security, Medical Center North Liberty, UI Health Care
Courtney Gent, Pharmacy Director, Department of Pharmaceutical Care, Medical Center North Liberty, UI Health Care
Terry Johnson, University Chief Financial Officer and Treasurer
Iowa Board of Regents
Office of Auditor of State

# North Liberty Hospital Building Access and Security

**BACKGROUND**

The UI Health Care Medical Center North Liberty (MCNL), located on a 60-acre campus at the intersection of Forevergreen Road and Highway 965 in North Liberty, opened on April 28, 2025. The 469,000-square-foot facility includes a three-level hospital connected to a five-level medical office building. Clinical and perioperative spaces include 84 exam rooms, 12 operating rooms, 2 procedure rooms, and 14 emergency care rooms. The hospital currently provides 36 private inpatient rooms, with capacity to add 12 additional rooms as future needs arise.

The Department of Orthopedics and Rehabilitation primarily operates out of MCNL, including University of Iowa (UI) Sports Medicine, a comprehensive physical therapy and rehabilitation gym, and the Orthopedic Injury Walk-In Clinic. The campus supports a range of non-surgical services such as ultrasound-guided injections, electromyography, bone health injections and infusions, as well as regenerative medicine. Additional on-site services include an emergency department, a 24-hour retail pharmacy, advanced diagnostic imaging, durable medical equipment, clinical laboratory services, a cafeteria, and other patient amenities.

Security and access control for the campus is managed by the MCNL Department of Safety and Security (DSS) in collaboration with their counterparts at the UI Health Care Medical Center University campus (MCU). The building access security program incorporates both electronic and physical controls, including 400 surveillance cameras, 19 security officers, 94 duress buttons, and approximately 400 electronic badge readers. The department utilizes multiple information technology (IT) systems to support building access and security, including KeyWatcher for physical key management, Victor Surveillance for surveillance camera operation, C-Cure for badge access control, Green Security for vendor representative management, and FastPass for emergency department visitor management.

**PURPOSE AND SCOPE**

The purpose of this audit was to evaluate MCNL security and access controls in place and determine whether the opportunity for improvement exists. The audit objectives were to evaluate whether MCNL:

- Physical and electronic building access controls and management processes are in place, effective and operate appropriately.
- Surveillance cameras operate appropriately.
- Safety and Security policies are appropriate and followed.
- Pharmacy access management processes function appropriately.

The audit scope included the MCNL building access and security processes as well as related data from April 28, 2025, to the present. No reportable findings were identified related to the MCNL pharmacy access management processes.

**DISCUSSION AND AUDIT RECOMMENDATIONS**

**1) Vendor Representative Building Access**

*Discussion* – Vendor representatives (vendors) are not consistently following the check-in process when arriving at MCNL, increasing the risk of unauthorized facility access. While onsite, an inquiry of five vendors determined that they had not checked in via the vendor management system (VMS), Green

Security. Check-in via the VMS is required for vendors at each MCNL visit as stated in the vendor handbook, "*All vendors must check in via the vendor registration system mobile app., upon each visit."*

*Audit Recommendation* – MCNL DSS should establish a plan to enforce the vendor check-in policy and routinely review the VMS check-in reports to identify vendors who are not checking in consistently. Violations should be documented in accordance with the vendor representative disciplinary process.

*Management's Action Plan* – MCNL leadership, in collaboration with MCNL DSS and UI Health Care Supply Chain management, will establish a comprehensive plan to enforce compliance with vendor policies. All vendors will receive detailed communication outlining updated vendor expectations, which include mandatory printed badges, daily check-in/check-out requirements, and other vendor access changes. Dashboards will be utilized to reconcile check-in data with vendor badge access to identify vendors not adhering to the vendor check-in policy. Monthly badge access reviews will be used to detect inactive or misused badges and ensure compliance with the designated entry point. Violations identified will be documented and addressed in accordance with the vendor representative disciplinary process. Compliance findings will also be shared during business reviews to reinforce expectations and maintain transparency.

*Individuals Responsible* – Director of Operations, Medical Center North Liberty, UI Health Care and Director, Supply Chain, UI Health Care

*Target Date* – May 2026

**2) Building Badge Access**
*Discussion* – Building badge access is not consistently removed when no longer needed, which increases the risk of inappropriate or unauthorized access. A review of 3,074 individuals with active MCNL building access identified 39 as having inappropriate access, indicating a gap in the automated access control that is supposed to disable badge access after an individual separates from employment. Additionally, there is not a regular process in place to review individuals with active building access.

*Audit Recommendation* – MCNL DSS should remove access from the badges identified. MCNL DSS should regularly review individuals with active MCNL building access to verify users continue to have a business need for access. Additionally, MCNL DSS should investigate the root cause for user accounts not automatically deprovisioning and take corrective action to ensure the process functions as intended.

*Management's Action Plan* – MCNL DSS will revoke active badge access for all users identified. MCNL DSS will also perform ongoing reviews of individuals with active badge access to ensure their access remains appropriate. In addition, MCNL DSS will collaborate with MCU Safety and Security and MCNL Human Resources to review the current deprovisioning processes, identify gaps in access control, and implement improvements to ensure timely and accurate removal of system access.

*Individuals Responsible* – Director of Operations, Medical Center North Liberty, UI Health Care and Director, Safety and Security, Medical Center University, UI Health Care

*Target Date* – May 2026

**3) Key Management**
*Discussion* – MCNL key management controls are not adequate, increasing the risk of unauthorized building access. KeyWatcher is the key management system used for housing and tracking access to

physical keys to sensitive areas. The provisioning and deprovisioning process for the KeyWatcher system requires supervisors or Human Resources to notify MCNL DSS to add or remove users' access. Management expects keys to be returned to the cabinet within 24 hours of being checked out. A review of the 136 active KeyWatcher user accounts identified 5 belonging to former employees. A physical inventory of 101 keys within the KeyWatcher cabinet was compared with a system report to determine if all the keys were accounted for, either physically present in the cabinet or currently checked out. All keys were accounted for except for 5 keys noted to be checked out for at least 55 days. Programming for automated notification of overdue keys is not in place and no regular review of overdue or checked-out keys occur. A review of the five checked out keys found that some may not need to be stored in the KeyWatcher cabinet.

*Audit Recommendation* – MCNL DSS should deactivate KeyWatcher user accounts belonging to former employees. A regular review of KeyWatcher user accounts should be performed. The manual deprovisioning process should be evaluated to identify and correct control gaps. MCNL DSS should evaluate if keys stored in the KeyWatcher cabinet are appropriate to store there or if they should be properly secured elsewhere, implement an overdue key notification logic to support timely follow-up, and regularly review system reports to monitor checked-out and overdue keys.

*Management's Action Plan* – MCNL DSS will coordinate with MCU Safety and Security to ensure inactive employee user accounts are removed promptly. MCNL DSS will also perform a monthly review of KeyWatcher user accounts in collaboration with MCNL Human Resources. In addition, MCNL DSS will partner with MCU Safety and Security to review the deprovisioning process and identify any gaps in access control. MCNL DSS will evaluate the keys that are appropriate for storage in the KeyWatcher cabinet and will implement overdue-key logic with customized thresholds for each key. MCNL DSS will generate and review KeyWatcher reports weekly to monitor both checked-out and overdue keys.

*Individuals Responsible* – Director of Operations, Medical Center North Liberty, UI Health Care and Director, Safety and Security, Medical Center University, UI Health Care

*Target Date* – May 2026

**4) Surveillance Camera Operations**

*Discussion* – Surveillance cameras are not consistently monitored in real time and procedures are not in place to regularly evaluate equipment malfunctions, increasing the risk of ineffective security video coverage. An on-site review of live camera feeds identified five that were inoperative. A camera status report from October 2025 was reviewed and identified 26 cameras that were inoperable or had an error status during the month of October. These reports are not currently monitored for timely resolution of camera performance issues or identification of systemic camera errors. When camera issues are identified, MCNL DSS notifies MCU Safety and Security. MCU determines whether to engage the vendor or use in-house technicians for diagnosis and repair. However, there is no formal plan or protocol that exists to address cameras that remain inoperative for extended periods.

*Audit Recommendation* – MCNL DSS should establish a routine review process for all MCNL surveillance cameras, including regular monitoring of camera status reports to identify any systemic camera errors, and develop a formal plan for situations where a camera is expected to be out of service for a duration that requires a backup solution.

*Management's Action Plan* – MCNL DSS will conduct weekly reviews of all surveillance cameras to identify any issues. Any concerns found will be documented and forwarded to a technician for resolution. In

addition, MCNL DSS will implement a structured review process that includes ongoing monitoring of camera status reports obtained from the Victor Surveillance software and develop a formal plan to address situations in which a camera is expected to be out of service for an extended period, including the use of appropriate backup solutions.

*Individuals Responsible* – Director of Operations, Medical Center North Liberty, UI Health Care and Director, Safety and Security, Medical Center University, UI Health Care

*Target Date* – May 2026

**5) Duress Button Testing**

*Discussion* – MCNL DSS does not conduct regular duress button testing, which increases the risk of undetected system failures. MCNL has 94 duress buttons strategically located throughout the hospital. Three duress buttons were successfully tested with each functioning properly. However, a plan to perform routine duress button testing is not currently developed.

*Audit Recommendation* – MCNL DSS should conduct regular testing of duress button operations to ensure the systems are working appropriately.

*Management's Action Plan* – MCNL DSS will test the duress buttons annually. Also, MCNL DSS is working with Engineering Services to evaluate the creation of a preventative maintenance plan within the WebTMA preventative-maintenance tracking system for future years.

*Individual Responsible* – Director of Operations, Medical Center North Liberty, UI Health Care

*Target Date* – May 2026

**6) MCNL Safety and Security Policies**

*Discussion* – MCNL DSS policies do not consistently reflect current MCNL practices, increasing the risk of utilizing improper procedures. Ten published policies were reviewed with MCNL DSS that noted six required revisions to align with MCNL current practices. Additional MCNL-specific policies remain unissued as they have not been finalized, approved, and published.

*Audit Recommendation* – MCNL DSS should review and revise policies to align with current MCNL practices. Incomplete MCNL-specific policies should be finalized, approved, and published. A regular review of policies should be established moving forward.

*Management's Action Plan* – MCNL DSS will review and update all safety and security policies to align with current practices, finalize and publish outstanding MCNL-specific policies, and implement a governance framework to establish a yearly review process.

*Individuals Responsible* – Director of Operations, Medical Center North Liberty, UI Health Care and Director, Safety and Security, Medical Center University, UI Health Care

*Target Date* – May 2026

**7) User Access**

*Discussion* – The user access deprovisioning processes for both the Victor Surveillance and FastPass visitor management systems are not functioning effectively, increasing the risk of unauthorized system access.

A review of the 14 MCNL Victor Surveillance active user accounts identified 1 associated with a former employee. Similarly, a review of the 23 FastPass active users found 3 belonging to former employees, including 2 whose employment ended in July 2025. Both systems rely on manual notifications of employment changes for provisioning and deprovisioning actions, creating a dependency that contributes to delays and inconsistencies in removing access.

*Audit Recommendation* – MCNL DSS should promptly deactivate all Victor Surveillance and FastPass user accounts belonging to former employees, implement regular reviews to ensure user access remains appropriate, and evaluate the current deprovisioning process to identify and implement controls to remove access when it is no longer needed.

*Management's Action Plan* – MCNL DSS will work with MCU Safety and Security to ensure all inactive employee user accounts for both the Victor Surveillance and FastPass systems are promptly removed. MCNL DSS will conduct monthly reviews of Victor Surveillance and FastPass user accounts in partnership with the MCNL Human Resources Department to verify ongoing user appropriateness. In addition, MCNL DSS will collaborate with MCU Safety and Security and MCNL Human Resources to review the current deprovisioning processes, identify gaps in access control, and implement improvements to ensure timely and accurate removal of system access.

*Individuals Responsible* – Director of Operations, Medical Center North Liberty, UI Health Care and Director, Safety and Security, Medical Center University, UI Health Care

*Target Date* – May 2026

**SUMMARY**

Management has been responsive to the recommendations made during the audit. The successful implementation of the audit recommendations will further strengthen the building access control environment. Internal Audit will initiate a follow-up in the fourth quarter of FY 2026 to verify corrective actions have been implemented.

Donald Ball, Auditor

Kip Druecker, Audit Manager

James Pitcher, Assistant Audit Director

Chad Sharp, Chief Audit Executive

BOARD OF REGENTS
Governing Iowa's Public Universities

## Office of Internal Audit

IOWA

# Red Card Administration

**April 22, 2026**

**Distribution List**
Barbara Wilson, President
Beth Goetz, Director of Athletics Chair
Lyla Clerry, Senior Associate Athletics Director for Compliance and Sports Performance
Andy Banse, Associate Athletics Director for Compliance
Kira Blum, Director of Sports Nutrition
Terry Johnson, University Chief Financial Officer and Treasurer
Iowa Board of Regents
Office of Auditor of State

# Red Card Administration

**BACKGROUND**

University of Iowa (UI) Athletics provides meals for its nearly 600 student athletes in the form of team meals, travel per diem, and limited funding for other meals. Red Card is a web-based application, powered by Red Card Athletics, used to distribute funds to athletes for meals and groceries at select locations in the Iowa City area. In FY 2025 UI Athletics expended more than $3.6 million on meals for student athletes, with over $1 million of this being routed through Red Card.

Funds are loaded to student athletes' accounts during their seasons by the respective team's director of operations, except for Olympic sports which are loaded by the Director of Sports Nutrition. Athletics Compliance staff administer fund loading during school break periods. Loaded funds are assigned to be used during designated time periods ranging from one day to one week. Funds do not rollover from one period to the next and expire if not used. Fund loading is managed via the Red Card Athletics web platform which is accessible to those granted access by Red Card.

Red Card Athletics invoices UI Athletics only for funds used by student athletes. Student athletes are educated that funds are only to be used for food purchases. Items such as durable goods, energy drinks, supplements, tobacco, and alcohol are prohibited. Red Card Athletics monitors transactions and flags prohibited item purchases for review by UI Athletics. UI Athletics reviews these transactions, notifies the student athlete of the prohibited use, and charges the prohibited purchases to the student athlete's university bill (U-bill).

**PURPOSE AND SCOPE**

The purpose of this audit was to provide reasonable assurance that controls are in place and operating as intended and to determine whether opportunities for improvement exist. The audit objectives were to verify:

- Roster information on the Red Card platform is complete, accurate, and aligned with official university records.
- Student athletes receive timely guidance regarding Red Card rules and appropriate use.
- Prohibited items are administered consistently in line with university policy.
- Red Card fund loading is administered consistently, within approved limits, and without overlapping other meal provisions.
- Red Card transactions are accurately invoiced.
- Red Card user access is appropriate and regularly reviewed.

The scope of this audit included processes, controls, and related transactions for Red Card Administration from fiscal year (FY) 2024 to the present. There were no reportable findings related to rules education, fund loading, or invoicing.

**DISCUSSION AND AUDIT RECOMMENDATIONS**

**1) User Access**

*Discussion* – Access to the Red Card Athletics web platform is not consistently reviewed and updated for changing roles within the department, resulting in former employees inappropriately retaining access. The Information Technology Enterprise Authentication, Authorization, and Access Policy states, *"Data*

*Custodians must periodically review user privileges and modify, remove, or deactivate accounts when roles change."*

UI Athletics users are set up with access including the ability to modify team rosters, load and edit funds, and view transaction statements among other administrative capabilities. The current process to create an Athletics staff user profile includes Athletics Compliance sending a request to Red Card Athletics to add the user. However, there is no regular review process to remove users once access is no longer needed. Review of users found 6 of 24 active users are former UI employees and should not have access. Three of these individuals have access to administer all UI teams.

*Audit Recommendation* – Management should remove unnecessary user access to the Red Card web platform. A process should be established for removing access when an individual no longer requires access. Regular Red Card access reviews should be performed to verify that access is properly managed.

*Management's Action Plan* – Management will work with Red Card to remove unnecessary user access to the Red Card web platform and implement a process to remove access from users when access is no longer required. Athletics Compliance will engage in a quarterly review process with Red Card of administrative users within Red Card platform.

*Individuals Responsible* – Director of Sports Nutrition; Associate Athletics Director for Compliance

*Target Date* – April 2026

**2) Roster Management**

*Discussion* – Team rosters on the Red Card Athletics web platform are not consistently reviewed or validated for accuracy, resulting in incorrect information on team rosters and increased risk of missed or incorrect billing. Comparison of student athlete profiles in Red Card to university records found 26 with incorrect or incomplete information. This included 14 profiles with incorrect student identification (ID) numbers, 6 instances of last names not matching university records, 4 profiles not including student IDs, and 2 athletes' profiles having swapped student IDs. Student IDs along with names are used to identify student athletes that are to be charged for prohibited items. The current process to create student athlete profiles includes Athletics Compliance sending all teams' roster information to Red Card Athletics, including student athlete names, university ID, email address, and sport. Rosters are also updated throughout the year as necessary. However, there is no regular monitoring to verify roster accuracy and completeness.

*Audit Recommendation* – Management should verify current roster listings in Red Card are accurate. Additionally, management should establish a procedure to regularly review profiles and verify that requests to create student profiles are accurately processed.

*Management's Action Plan* – Management will work with Red Card to ensure current profile identifying information matches university records. A quarterly review process of student athlete and manager profile data will be conducted by the Compliance Office to reconcile data within the Red Card and university system.

*Individuals Responsible* – Director of Sport Nutrition; Associate Athletics Director for Compliance

*Target Date* – April 2026

**3) Prohibited Items**

*Discussion* – Charge monitoring processes do not consistently identify all transactions with prohibited items, resulting in prohibited item costs not being recovered. The Iowa Sports Nutrition's policy states, *"Student-athlete will receive a written notification, and their U-Bill account will be charged for any impermissible purchase."* Iowa Sports Nutrition downloads monthly Red Card reports identifying transactions with prohibited items purchased by student athletes. Transactions with prohibited items identified from the Red Card data report are manually entered one-by-one into the body of an email to Athletics Business Operations. The Red Card data report is also attached. Athletics Business Operations then applies these prohibited item charges to student athletes' U-bills. Review found three instances of prohibited item transactions that were not charged to a student athlete's U-bill.

*Audit Recommendation* – Management should charge students for the identified unbilled prohibited item costs and re-evaluate the Red Card charge monitoring process to more consistently identify all prohibited items.

*Management's Action Plan* – Management will charge students for identified unbilled prohibited items. Management will verify the prohibited items report for accuracy with Red Card before preparing the email summary report for the business office and sending individual student athlete email notifications. The summary email sent to the business office will be reformatted so that charges to students are easily identifiable. In addition, the finance office will send a monthly U-bill charge report to Sports Nutrition staff for review. Any missed charges will be reconciled at the end of each semester.

*Individual Responsible* – Director of Sports Nutrition

*Target Date* – April 2026

**SUMMARY**

Management has been responsive to the recommendations made during the audit. The successful implementation of the audit recommendations will further strengthen the control environment. Internal Audit will initiate a follow-up in the fourth quarter of FY 2026 to verify corrective actions have been implemented.

Mike Cahill, Auditor

James Pitcher, Assistant Audit Director

Chad Sharp, Chief Audit Executive

BOARD OF REGENTS
Governing Iowa's Public Universities

## Office of Internal Audit

IOWA

## Research Integrity and Security Office

**April 22, 2026**

**Distribution List**
Barbara Wilson, President
David Schwebel, Vice President for Research
Jennifer Lassner, Associate Vice President, Office of the Vice President for Research
Mike Andrews, Director of Research Integrity and Security, Office of the Vice President for Research
Kevin Zihlman, Associate Director of Research Integrity and Security, Office of the Vice President for Research
Terry Johnson, University Chief Financial Officer and Treasurer
Iowa Board of Regents
Office of Auditor of State

# Research Integrity and Security Office

**BACKGROUND**

The Research Integrity and Security Office (RISO), within the Office of the Vice President for Research (OVPR), supports the research enterprise at the University of Iowa by promoting ethical, secure, and compliant research practices. The RISO monitors training completion of the Responsible Conduct of Research (RCR), Responsible and Ethical Conduct of Research (RECR), and Research Security, which are all completed through the Collaborative Institutional Training Initiative program. RCR training is required for research funded by the National Science Foundation (NSF), National Institutes of Health (NIH), U.S. Department of Agriculture, and National Institute of Food and Agriculture. RECR training is required by research funded through the NSF as part of the Creating Helpful Incentives to Produce Semiconductors and Science Act of 2022. Research Security training is required by the NSF, NIH, Department of Energy and the Department of Defense for researchers submitting funding proposals. International Travel Security is one of the four research security program standard components mandated by the federal Office of Science and Technology Policy (OSTP). International travel training was created by the RISO to fulfil this requirement for international travelers who have a research related purpose as part of the reason for travel. Other responsibilities include investigating potential research misconduct or security risks, maintaining documentation related to federal compliance requirements, and reviews of foreign talent recruitment programs. Currently, RISO staffing consists of two full-time employees and one part-time employee.

RISO utilizes two research-related applications, Proofig and iThenticate. Proofig is used exclusively by RISO to assess potential image manipulation during applicable research misconduct investigations. iThenticate is available to researchers across the university, with the license primarily funded by the OVPR. Researchers use iThenticate to identify potential plagiarism concerns prior to publication, while RISO uses the tool to review plagiarism allegations associated with reported misconduct cases.

**PURPOSE AND SCOPE**

The purpose of this audit was to evaluate the effectiveness of the RISO's controls and determine if they are operating as intended. The specific objectives included verifying whether:

- Compliance processes are in place for identifying, implementing, and monitoring federal agency requirements.
- RISO-related committees and working groups maintain appropriate documentation.
- Research misconduct investigation processes are established and appropriate.
- International travel training processes are operating effectively.
- Foreign talent recruitment program processes identify researcher participation and maintain appropriate documentation.
- Research compliance reporting is accurate, and access is appropriately restricted.
- Proofig and iThenticate systems are properly managed and maintained.

The audit scope included current processes, controls, and related data from fiscal year (FY) 2026 to the present. There were no reportable findings related to committees and working groups, research misconduct investigation processes, foreign talent recruitment programs, research compliance reporting, and the Proofig and iThenticate systems.

**DISCUSSION AND AUDIT RECOMMENDATIONS**

**1) RISO Change Management Procedures**

*Discussion* – There are no formally documented procedures for RISO's internal change management processes, increasing the risk of inconsistent implementation of federal requirements. When federal requirements change, the RISO updates internal procedures to remain compliant with funding agency requirements, including revisions to policies, researcher training requirements, and reporting obligations to federal agencies. However, there are currently no documented procedures to monitor, document, review, and maintain a history of these internal updates.

*Audit Recommendation* – Management should implement and document change management procedures to review, document, apply, and communicate changes to federal agency requirements to the research community.

*Management's Action Plan* – RISO will develop a desk procedure outlining how policies and procedures are updated in response to regulatory changes. Additionally, RISO will implement timestamping of all policy and procedural documents to document updates and demonstrate ongoing review. Staff, researchers, and the associate deans for research and faculty will be informed of changes through newsletters, researcher outreach, Research Council discussions, OVPR Researcher newsletter updates, and website updates.

*Individual Responsible* – Director of Research Integrity and Security, Office of the Vice President for Research

*Target Date* – January 2027

**2) International Travel Training Procedure**

*Discussion* – The international travel training material does not have a formally documented review process, increasing the risk of outdated training content. The purpose of the internally developed training is to comply with the international travel security program standard mandated by the OSTP and raise awareness of the risks associated with international travel. The RISO developed this material in the fall of 2025 with training required once within a 12-month period for travelers who have a research related purpose as part of their reason for travel. However, there is no documented process in place for periodic review to verify that training material continues to align with current institutional guidance.

*Audit Recommendation* – Management should formalize a documented process for reviewing and updating international travel training material.

*Management's Action Plan* – On an annual basis the RISO will review the International Pre-Travel Training content to determine whether updates are needed. If changes in federal regulations or institutional policies occur that impact the training, RISO will coordinate with the appropriate offices to update the materials in a timely manner and record when those changes occur.

*Individual Responsible* – Director of Research Integrity and Security, Office of the Vice President for Research

*Target Date* – January 2027

**SUMMARY**

Management has been responsive to the recommendations made during the audit. The successful implementation of the audit recommendations will further strengthen the control environment. Internal Audit will initiate a follow-up in the third quarter of FY 2027 to verify corrective actions have been implemented.

Gavin Macdonald, IT Auditor

Kip Druecker, Audit Manager

James Pitcher, Assistant Audit Director

Chad Sharp, Chief Audit Executive

BOARD OF REGENTS
Governing Iowa's Public Universities

## Office of Internal Audit

IOWA

# Women's Resource and Action Center

**April 22, 2026**

**Distribution List**
Barbara Wilson, President
Sarah Hansen, Vice President, Division of Student Life
Scott Seagren, Chief Financial Officer, Division of Student Life
Maria Bruno, Assistant Vice President, Division of Student Life
Linda Kroon, Director, Women's Resource and Action Center
Terry Johnson, University Chief Financial Officer and Treasurer
Iowa Board of Regents
Office of Auditor of State

# Women's Resource and Action Center

**BACKGROUND**

The Women's Resource and Action Center (WRAC) is a non-revenue producing department within the Division of Student Life that is funded by five gifts and the general education fund. The department has eight employees and administers several programs including Iowa National Education for Women (N.E.W) Leadership, Weaving our Community Network, and Night Slice. WRAC also offers violence prevention training, space reservation, and counseling services to University of Iowa faculty, staff, students and the surrounding community.

WRAC's counseling services are provided for free by doctoral students from several academic programs who are performing their practicum. WRAC has three student counselors that rotate in and out each academic year. Counseling note review and advisement is provided by the student counselors' academic program outside of WRAC. Titanium is the software used to schedule counseling appointments and record session notes. Access to Titanium is granted and removed by the WRAC director when counselors change each academic year.

The Jeanne Clery Campus Safety Act (Clery Act) requires universities receiving federal funding to maintain and report crime information on or near their respective campus. As WRAC is a confidential source on campus at the University of Iowa, it is only required to report limited information from reportable incidents. WRAC counselors are licensed practitioners or are working under a licensed practitioner, so information shared during sessions is not required to be reported. However, any instances reported to the WRAC director must be reported for Clery compliance as the WRAC director is not a licensed counselor and is a Campus Security Authority (CSA). As a CSA, the WRAC director has a legal obligation to report all known criminal incidents occurring on campus or during university activities to the Office of Clery Compliance.

**PURPOSE AND SCOPE**

The purpose of this audit was to provide reasonable assurance that controls are in place and operating as intended and to determine whether opportunities for improvement exist. The audit objectives were to verify:

- Purchases and gifts are administered in accordance with university and donor requirements.
- Monthly Account Statement reconciliations are performed timely, in accordance with university policy, and processes are documented.
- A business continuity plan is documented, reviewed, and updated on a regular basis.
- Training is appropriately assigned and completed in compliance with university requirements.
- The institutional contract with the Domestic Violence Intervention Program (DVIP) and Rape Victim Advocacy Program (RVAP) is current, signed by appropriate parties, and terms are followed.
- Mandated reporting is completed in compliance with the Clery Act.
- Physical and system access is appropriate and reviewed regularly.

The audit scope included WRAC procedures, controls, and related transactions from fiscal year (FY) 2025 to the present. There were no reportable findings related to procurement card purchases, monthly account statement reconciliations, required training, and the institutional DVIP and RVAP contract.

**DISCUSSION AND AUDIT RECOMMENDATIONS**

**1) System Access**

*Discussion* – Shared drive access is not regularly reviewed, and the WRAC director has a dual role as both a Campus Security Authority (CSA) and the Titanium system administrator, increasing the risk for inappropriate access and untimely required Clery incident reporting. IT Security Policy (IT-15) - Enterprise Authentication, Authorization, and Access Policy states, *"Data Custodians must periodically review user privileges and modify, remove, or deactivate accounts when roles change. Data stewards will define the review period in conjunction with data custodians."* Review of accounts with access to the shared drive found nine individuals no longer affiliated with WRAC that continue to have access.

As the Titanium system administrator, the WRAC director has access to counseling notes even though it is not required in the performance of her duties. Titanium system functionality does not allow access to review counseling notes to be decoupled from the ability to manage system access. As the WRAC director is a CSA while not being a licensed counselor, she is required to report Clery incidents noted within counseling notes that she reviews.

*Audit Recommendation* – WRAC management should remove unnecessary access to the WRAC shared drive. A process should be established for removing an individual's access when they change roles or leave the department. Regular reviews should be established to verify access is properly maintained. Additionally, WRAC management should work with the Office of General Counsel, the Information Security and Policy Office, and the Office of Clery Compliance to re-evaluate the Titanium access and system administration while ensuring compliance with the Clery Act.

*Management's Action Plan* – WRAC management will work with WRAC IT staff to grant access to appropriate users and remove access to individuals who are no longer with WRAC. The WRAC Director will review access at the end of each academic term and communicate necessary changes to IT staff. WRAC's Titanium system will be merged into the University Counseling Service's (UCS) instance of Titanium during Summer 2026, in preparation for UCS staff to manage going forward. The system administrator will be the UCS clinical director, who is a licensed mental health clinician.

*Individual Responsible* – Director, Women's Resource and Action Center

*Target Date* – July 2026

**2) Gift Fund Accounting**

*Discussion* – Gift expenses cannot be traced to specific gifts, increasing the risk of inappropriate spending or misappropriated funds. Of WRAC's five gifts, three are restricted for Iowa N.E.W Leadership program purposes and are accounted for in one general ledger account. Of these three, one is further restricted to support an annual keynote for the Iowa N.E.W. Leadership program. When multiple gifts are associated with only one general ledger account, it creates monitoring limitations of gift expenses as reviewers cannot determine what expenses connect to which gift. In addition to the general ledger, WRAC uses the University of Iowa Center for Advancement (UICA) to track balances for individual gifts.

*Audit Recommendation* – WRAC management should work with the Controller's Office to set up an individual general ledger account for the Keynote Address gift.

*Management's Action Plan* – WRAC management will create a new restricted gift account to separately track restricted fund transactions for the Iowa N.E.W. Leadership Keynote Address and connect it with the

corresponding UICA fund. This will be a separate general ledger account from the existing Iowa N.E.W. Leadership program restricted gift account.

*Individual Responsible* – Director, Women's Resource and Action Center

*Target Date* – Closed

**3) Night Slice Memorandum of Understanding**

*Discussion* – The memorandum of understanding (MOU) with Papa Johns that defines the Night Slice program was not properly approved, increasing the risk for mishandled or misappropriated funds. During each fall semester, the Night Slice program offers slices of pizza to college students on weekend nights as an alternative to drinking. From midnight to 2:00 am on Friday and Saturday nights, students can show their university identification card at Papa Johns as payment for two slices of pizza with a limit of up to 200 students per night. The Iowa Policy Manual 11.4 Signatory Authority states, *"The President has delegated contracting authority to the Chief Procurement Officer for purchase orders and purchase contracts."* The MOU between WRAC and Papa Johns to provide this service was not reviewed and approved by the Chief Procurement Officer as required.

*Audit Recommendation* – WRAC management should work with Purchasing to review and appropriately approve the MOU with Papa Johns.

*Management's Action Plan* – WRAC management will work with Purchasing to create an approved MOU if funding is received to continue the program. If funding is not received, the program will end, and no MOU will be needed.

*Individual Responsible* – Director, Women's Resource and Action Center

*Target Date* – July 2026

**4) Physical Access**

*Discussion* – Physical access is not regularly reviewed and a physical key inventory does not exist, increasing the risk of inappropriate access. External doors to the WRAC building are secured using the AMAG electronic badge access system. WRAC has 4 AMAG badge access groups and within those access groups 41 individuals have 24/7 access to WRAC's building that do not have a connection to WRAC. Of these 41 individuals, 2 have left the university. Additionally, WRAC has physical keys for doors and cabinets within the building that are stored in an unlocked drawer in the operations and administration coordinator's desk. There is no physical key inventory or check-in/checkout process.

*Audit Recommendation* – WRAC should remove AMAG access to individuals without an appropriate need. WRAC should create and maintain a key inventory that assigns each key to a keyholder and create a check-in/checkout process to monitor key distribution.

*Management's Action Plan* – Management will inventory all keys and records will be maintained on an ongoing basis by the Administrative Services Coordinator. Keys will be stored in a locked key case and kept in a secure location. AMAG access will be reviewed at least monthly by the Administrative Services Coordinator and Director, and access will be removed for individuals once there is no longer a business need. The Director and Administrative Services Coordinator have the authority to request that physical access be changed for individuals by the Security Engineering Services team.

*Individual Responsible* – Director, Women's Resource and Action Center

*Target Date* – April 2026

**5) Training**

*Discussion* – Family Educational Rights and Privacy Act (FERPA) training has not been consistently assigned or completed, increasing the risk that employees are unaware of regulations and related information. A review of required training completion found one WRAC employee not current with FERPA training and four student employees who have never completed FERPA training. The Office of the Executive Vice President and Provost Updated FERPA Compliance Requirements state, *"All University of Iowa faculty, teaching assistants, and staff who many interact or work with students and/or student records will be required to complete FERPA training every three years."* The positions that these non-compliant individuals hold have not been properly assigned FERPA training within the Compliance and Qualifications (CQ) system. Not being assigned FERPA training in CQ results in automated reminders not being sent to complete upcoming required FERPA training.

*Audit Recommendation* – WRAC management should work with employees to ensure required trainings are completed. Management should also work with HR to review job responsibilities and to ensure all individuals are properly assigned necessary training. Completion of training should be monitored going forward.

*Management's Action Plan* – WRAC Director will manage and monitor non-student staff completions of required trainings, and the Violence Prevention Program Coordinator will manage and monitor student staff completion of required trainings. WRAC will work with HR to assign required FERPA training to staff.

*Individual Responsible* – Director, Women's Resource and Action Center

*Target Date* – April 2026

**6) Business Continuity Plan (BCP)**

*Discussion* – WRAC does not have a BCP, increasing the risk that activities will not be able to be resumed in the event of an emergency. A BCP encompasses activities necessary for the department to return to normal activities in the event of an emergency such as a cyber security event or natural disaster. The IT Security Policy states, *"The Data Steward will…ensure implementation of policies, and documentation of process and procedure for guaranteeing availability of systems, including…disaster recovery, business continuity…"* The IT Security Policy defines a data steward as *"the senior official within a college or departmental unit accountable for managing information assets."* The University of Iowa has a subscription to Kuali Ready that assists units in creating departmental plans for continuity of operations, including BCPs. Annual automated reminders to update BCPs will also be sent to departments that have created their BCP using Kuali Ready.

*Audit Recommendation* – WRAC should develop a BCP using the Kuali Ready system. A regular review process should be implemented to ensure updates are made timely.

*Management's Action Plan* – WRAC management will work with Risk Management, Insurance, and Loss Prevention to create a business continuity plan for WRAC.

*Individuals Responsible* – Director, Women's Resource and Action Center and Assistant Director, Women's Resource and Action Center

*Target Date* – July 2026

**SUMMARY**

Management has been responsive to the recommendations made during the audit. The successful implementation of the audit recommendations will further strengthen the control environment. Internal Audit will initiate a follow-up in the first quarter of FY 2027 to verify corrective actions have been implemented.

Sydney Steffen, Auditor

James Pitcher, Assistant Audit Director

Chad Sharp, Chief Audit Executive


**Office of Internal Audit**


# UNI Works

**April 22, 2026**

**Distribution List**
Mark Nook, President
Michael Hager, Senior Vice President for Finance and Operations
Karmen Dillon, Chief Information Officer
Christina Geweke, Assistant Vice President for Business Operations
Jason Ebensberger, System Application Administrator, Information Technology
Kevan Forest, IT Administrator, Information Technology
Iowa Board of Regents
Office of Auditor of State

# UNI Works

**BACKGROUND**

UNI Works is the University of Northern Iowa's enterprise-level cloud-based Workday solution, implemented to replace the legacy server-based Oracle E-Business platform. UNI Works represents a major investment which supports modernization of Human Resources, payroll, and workforce operations by providing a unified platform accessible to faculty, staff, and student employees across campus. The implementation, completed over an 18-month period, required significant institutional resources, including participation from nearly 150 university personnel and external consultants to complete system configuration and testing. The system went live on July 1, 2024 and continues to receive biannual Workday updates.

**PURPOSE AND SCOPE**

The purpose of the audit was to evaluate the adequacy and efficiency of significant operational processes for UNI Works and to provide reasonable assurance that internal controls are in place and operating as intended. The objectives of the audit were to assess:

- The effectiveness of UNI Works governance and oversight structures.
- Alignment of UNI Works capabilities with institutional strategy and value-realization goals.
- The operational efficiency of key UNI Works processes and support functions.
- Adequacy of UNI Works security and internal control practices.
- The effectiveness of licensing management processes of Workday for cost optimization.

The audit scope included UNI Works business processes, information, and related transactions from July 1, 2024 to the present.

**DISCUSSION AND AUDIT RECOMMENDATIONS**

**1) Audit Logging, Monitoring & Suspicious Activity Response**

*Discussion* – Insufficient audit configuration, limited log retention, and the absence of a formal process for managing suspicious activity reduces the institution's ability to promptly detect and effectively respond to issues, as well as maintain strong compliance and risk oversight. Workday audit logging and monitoring practices are not formally governed or consistently configured, as logs are reviewed only on an ad hoc basis during troubleshooting, with no defined review cadence, assigned ownership, or documented responsibilities. No structured process for identifying, escalating, investigating, and documenting suspicious activity exists, which limits the ability to detect or respond to security concerns. The system relies on the default "all-or-nothing" auditing and does not use Audit Tags to capture detailed changes to high-risk business objects, reducing visibility into critical system modifications. Additionally, user activity and integration logs are retained for only 30 days, which may not meet investigative or compliance requirements.

*Audit Recommendation* – Management should establish a formal Workday audit logging and monitoring program that sets ownership, periodic review procedures, escalation protocols, extended log retention, and application of Audit Tags to ensure timely detection, investigation, and oversight of suspicious or unauthorized activity.

*Management's Action Plan* – Management will establish a formal Workday audit logging and monitoring program to improve the university's ability to detect, review, and respond to system activity. Initial efforts will focus on putting a basic structure in place, including defining ownership across Information Technology and functional areas, setting a consistent review cadence for high-risk activity, and documenting procedures for identifying, escalating, and investigating suspicious or unauthorized activity.

As part of this work, management will evaluate current audit configurations and log retention, implement Audit Tags for high-risk business objects, and align practices with institutional security standards. After this baseline structure is established in fiscal year (FY) 2026, management will continue to mature the program in FY 2027 by refining processes, expanding monitoring capabilities, and strengthening documentation to support ongoing oversight and compliance.

*Individual Responsible* – Chief Information Officer

*Target Date* – July 2026

**2) Access Governance and Segregation of Duties**
*Discussion* – Excessive System Administrator access and broad Payroll Administrator privileges create a segregation-of-duties weakness, further compounded by the lack of a formal, periodic review of Workday security roles and assignments, increasing the risk of unauthorized or inaccurate transactions. The System Administrator role can self-assign to the Payroll Partner group and the Payroll Administrator group retains extensive rights, including modifying payroll inputs, initiating and approving payroll processes, and performing critical tasks such as Run Pay Calculation, Run Manual Payment, and Assign Pay Groups. Concentrating these capabilities within one security group increases the risk of unauthorized or inaccurate payroll activity.

*Audit Recommendation* – Management should implement independent approval for all Payroll Partner and privileged role assignments, restrict excessive System Administrator access, and segregate payroll responsibilities into distinct roles; Payroll Data Entry (initiate/modify), Payroll Approval (approve only), and Payroll Execution (run calculations and payments). A formal, periodic review of payroll-related security roles should be established to ensure ongoing segregation-of-duties compliance.

*Management's Action Plan* – System Administrator access will be reviewed and adjusted to align with least-privilege principles, and payroll-related access will be restructured to reduce concentration of duties, as possible. Management will also establish a formal, recurring access-review process in coordination with HR, Payroll, and IT Security to ensure roles and assignments remain appropriate over time. Initial role updates and approval workflows will be implemented in FY 2026, with ongoing reviews continuing thereafter.

*Individuals Responsible* – Chief Information Officer and Assistant Vice President for Business Operations

*Target Date* – July 2026

**3) Workday Governance, Procedures and Training Oversight**
*Discussion* – The Workday program lacks formal strategic direction, governance, and decision-making structures, with undocumented business processes and key performance indicators (KPIs), resulting in inconsistent practices, limited accountability, and reduced oversight effectiveness. The current governance structure remains informal and is based on the vendor's initial implementation framework. The institution has not established official governance objectives; decision-making authority, defined

roles, or responsibilities. Governance committees meet only on an ad hoc basis without agendas, documented decisions, or formal oversight expectations. Business procedures are not centrally maintained with version control, leading to reliance on informal knowledge and inconsistent workflows. Training requirements are not systematically enforced, leaving mandatory training overdue with no monitoring mechanism.

Additionally, KPIs for system effectiveness, such as processing accuracy, ticket-resolution timeliness, audit-review completion, and training adherence, have not been clearly defined or consistently tracked. The absence of measurable performance data limits leadership's ability to adequately assess operational efficiency, identify emerging risks, and ensure the system is being managed in alignment with institutional expectations.

Although implementation progress is tracked through a project tracker, this does not function as a strategic governance structure to sufficiently support effective long-term system management or alignment with institutional priorities. The absence of a formal governance model reduces accountability, weakens structure, and limits the institution's ability to manage Workday effectively.

*Audit Recommendation* – Management should establish and formally approve a comprehensive Workday governance and strategic framework that includes a documented strategic plan, governance charter, and clear decision-making structure. The framework should standardize and maintain authoritative business process procedures, define role-based training requirements, implement centralized training oversight with tracking and monitoring of mandatory completion, and incorporate defined KPIs to ensure accountability, consistency, effective system oversight, and measurable operational performance.

*Management's Action Plan* – Management will formalize a comprehensive Workday governance framework to establish clear structure, accountability, and oversight for long-term system management. This will include finalizing and implementing a governance charter, defining decision-making structures, and clearly assigning roles and responsibilities.

As part of this effort, management will establish consistent governance forums with defined meeting cadences and documentation of decisions, standardize and centrally maintain business process procedures, and implement role-based training requirements with centralized tracking and monitoring. Management will also define and begin tracking KPIs to measure operational effectiveness and support ongoing oversight. This work builds on the draft governance framework already developed and shared during the audit process and will be implemented in phases beginning in FY 2026, with continued maturation over time.

*Individual Responsible* – Chief Information Officer

*Target Date* – October 2026

**4) Business Continuity and Disaster Recovery (BCDR)**
*Discussion* – The institution lacks Workday specific BCDR documentation, potentially limiting its ability to respond effectively to disruptions affecting business operations. The institution currently relies entirely on Workday's vendor-provided continuity capabilities and does not maintain an internal Workday specific BCDR plan that outlines institutional roles, internal dependencies, recovery priorities, or operational response procedures during a service disruption. Without defined recovery expectations or documented workflows, the institution may be unable to effectively manage disruptions that impact critical academic,

administrative, or regulatory operations. This lack of planning increases the risk of prolonged downtime, delayed recovery actions, and misalignment with regulatory or institutional continuity requirements.

*Audit Recommendation* – Management should develop and formally approve Workday-specific BCDR documentation defining recovery requirements, roles, dependencies, and escalation procedures. Periodically test the plan in coordination with Workday to ensure alignment with institutional continuity needs.

*Management's Action Plan* – Management will develop and formalize Workday-specific BCDR documentation to define institutional roles, dependencies, recovery priorities, and escalation procedures. This work will be coordinated with central IT disaster recovery planning and aligned with Workday vendor capabilities to ensure a consistent and practical approach to service disruption response. Periodic testing, including tabletop exercises, will be conducted to validate readiness and alignment with institutional continuity expectations. Discovery will be implemented in phases beginning in FY 2026, with continued maturation over time and integration of related operational oversight activities.

*Individual Responsible* – Chief Information Officer

*Target Date* – January 2027

**5) Workday Issue Tracking**

*Discussion* – Workday-related issues are not adequately monitored and governed, resulting in unresolved backlogs, unclear ownership, and inconsistent resolution timelines. Workday-related issues tracked through the JIRA software are currently managed by the Workday implementation team and are not subject to effective centralized monitoring or oversight, leading to numerous unresolved, unassigned, or overdue tickets that fail to meet service level expectations. Documented procedures, clear ownership, or structured escalation requirements for issue tracking have not been established, which increases the risk that systematic issues, particularly those affecting payroll, financial processes, or data integrity may remain unaddressed. This lack of oversight reduces accountability, delays resolution, and increases the likelihood that operational or system issues could have broader downstream impacts.

*Audit Recommendation* – Management should establish centralized issue monitoring with documented procedures, clear ownership, service level agreement enforcement, periodic management review, and escalation pathways to ensure timely and accountable resolution of system issues.

*Management's Action Plan* – Management will establish centralized governance and oversight for Workday issue tracking to improve visibility, accountability, and timely resolution of system issues. This will include defining clear ownership, documenting standard procedures, establishing service level expectations, and implementing escalation pathways for unresolved or high-risk issues. Workday issue tracking will be aligned with institutional service management practices, including regular reporting and management review of backlog, aging, and resolution performance. Discovery will begin in FY 2026, with initial documentation and plan approval continuing into FY 2027, followed by ongoing review and refinement thereafter.

*Individual Responsible* – Chief Information Officer

*Target Date* - April 2027

**6) Licensing Value Assurance**

*Discussion* – No process exists for regular assessment of the Workday Master Agreement licensed module utilization, limiting optimization and opportunities for cost savings. The ten-year bundled Workday Master Subscription Agreement establishes fixed subscription fees based on total employee count rather than module utilization. Several bundled modules are scoped out of the implementation and are not actively utilized yet remain included within the contracted subscription. The initial implementation plan determined modules that would be activated and established structures for usage. However, since implementation, no comprehensive analysis has occurred of the licensed modules against strategic institutional initiatives or existing software contracts to determine if process efficiencies or cost savings exist.

*Audit Recommendation* – Management should establish a process for regular review of all licensed modules. Reviews should assess the capabilities of licensed modules against the strategic needs of the institution and compare Workday capabilities against all existing software contracts to determine opportunities for Workday optimization. Additionally, in coordination with Purchasing, a process should be developed and implemented that prioritizes usage of licensed Workday modules over external software contracts.

*Management's Action Plan* – Management will develop and implement a process to evaluate Workday licensed modules against institutional needs and current system utilization based on strategic direction provided by senior leadership. This process will support both review of existing applications and evaluation of new software purchases to ensure Workday capabilities are considered where appropriate. This process will be supported by development of an inventory of Workday-enabled functionality to inform review of future software purchase requests, as well as an inventory of existing institutional applications to identify opportunities where functionality may be consolidated or migrated to Workday when appropriate. Discovery will begin in FY 2027, with initial documentation and process implementation following and ongoing review and refinement thereafter.

*Individual Responsible* – Chief Information Officer

*Target Date* - April 2027

**7) Third-party Oversight and System and Organization Controls (SOC) Review**

*Discussion* – Lack of a formal process for SOC report reviews and inadequate documentation of the third-party lifecycle access review, increases vendor-related security and compliance risks. Formal procedures for reviewing SOC 1 or SOC 2 reports from third-party service providers do not exist and no structured process for evaluating findings, documenting assessments, or tracking remediation actions is maintained. Similarly, no formalized process governing the provisioning, monitoring, or deprovisioning of implementer or third-party accounts exists, increasing the risk of unauthorized access or unmonitored system activity by external users. Without defined procedures, third-party oversight is inconsistent and incomplete, elevating compliance, security, and operational risks associated with vendors and external support personnel.

*Audit Recommendation* – Management should establish documented procedures for SOC report review including evaluation criteria, documentation requirements, tracking of remediation actions, and formalize provisioning, reviewing, and deprovisioning procedures for implementer accounts.

*Management's Action Plan* – Management will develop and implement formal procedures for third-party oversight, including the review of SOC 1 and SOC 2 reports. This will include establishing evaluation

criteria, documentation standards, and a process for recording assessments and tracking any remediation actions identified through SOC report review. In addition, procedures will be established to govern the provisioning, monitoring, periodic review, and deprovisioning of third-party and implementer access to ensure appropriate oversight of external users. These practices will be aligned with institutional vendor management and information security standards. Discovery will begin in FY 2026, with initial documentation and process implementation following and continued review and refinement thereafter.

*Individual Responsible* – Chief Information Officer

*Target Date* - October 2026

**SUMMARY**

Management has been responsive to the recommendations made during the audit. The successful implementation of the audit recommendations will further strengthen the control environment. Internal Audit will initiate a follow-up in the fourth quarter of FY 2027 to verify corrective actions have been implemented.

Vallarie Hope, Senior Auditor

Joshua Randall, Assistant Audit Director

Chad Sharp, Chief Audit Executive

BOARD OF REGENTS
Governing Iowa's Public Universities

**Office of Internal Audit**

2100-01 University Capitol Centre
201 S. Capitol St.
Iowa City, Iowa 52242-5500

# UNIVERSITY OF IOWA
# AUDIT FOLLOW-UP
# M E M O R A N D U M

TO: J. Joshua Wilda, Associate Vice President for Information Systems and Chief Information Digital Officer, UI Health Care
Teresa Franklin, Senior IT Director, Communication and Collaboration Services, HCIS

FROM: Gavin Macdonald, IT Auditor
Kip Druecker, Audit Manager
James Pitcher, Assistant Audit Director
Chad Sharp, Chief Audit Executive

DATE: April 22, 2026

SUBJECT: Epic Secure Chat

The Epic Secure Chat audit report was issued on September 17, 2025. A follow-up review has been conducted to assess management's progress in implementing the corrective actions identified in the original report.

**Nurse Call Integration** – Management implemented Epic's native voice over internet protocol solution allowing the nurse call system to integrate directly with Epic applications. All Voalte telephone numbers were transferred over to the Epic environment allowing the decommission of the Voalte application.

The audit is now closed.

cc: Barbara Wilson, President
Denise Jamieson, Vice President for Medical Affairs and Dean of Carver College of Medicine
Brad Haws, Chief Executive Officer, Clinical Enterprise, Associate Vice President, UI Health Care
Mark Henrichs, Associate Vice President for Finance and Chief Financial Officer, UI Health Care
Brad Rohrer, Associate Vice President and Chief Information Officer, ITS
Zach Furst, Chief Information Security Officer, Information Security & Policy Office, ITS
Alison Bronson, Director of Clinical Informatics, HCIS
Terry Johnson, University Chief Financial Officer and Treasurer
Iowa Board of Regents
Office of Auditor of State

BOARD OF REGENTS
Governing Iowa's Public Universities

Office of Internal Audit
2100-01 University Capitol Centre
201 S. Capitol St.
Iowa City, Iowa 52242-5500

**UNIVERSITY OF IOWA**
**AUDIT FOLLOW-UP**
**M E M O R A N D U M**

TO: Lauren Lessing, Executive Director, Stanley Museum of Art

FROM: Mike Cahill, Auditor
James Pitcher, Assistant Audit Director
Chad Sharp, Chief Audit Executive

DATE: April 22, 2026

SUBJECT: Stanley Museum of Art

The Stanley Museum of Art audit report was issued on September 17, 2025. A follow-up review has been conducted to assess management's progress in implementing the corrective actions identified in the original report.

**Donated Art Valuation** – Internal curators are now being used to obtain timely estimated values of donated art that is received without valuation documentation. Donated art acquisitions valued over $5,000 are reported via Capital Asset Management's Addition Request e-form by the end of the fiscal year. Additionally, the Stanley Museum of Art Collections Management Policy has been updated to describe donation valuation, accessioning, and reporting processes.

**Art Inventory** – The number of items not inventoried within the last five years has been significantly reduced. In 2025, 29% of the art pieces were inventoried, a significant increase from an average of 14% during each of the previous four years. The museum will continue to inventory at least 20% of its inventory per year to comply with its policy of having all items inventoried within a 5-year period.

**System Security Reviews** – The Asana and Doubleknot systems were submitted to the Information Security and Policy Office for security review.

**Required Training** – All employees who handle cash or cash equivalents have been assigned and have completed required trainings.

Management has been proactive in addressing each of the original recommendations. The audit is now closed.

cc: Barbara Wilson, President
Kevin Kregel, Executive Vice President and Provost
Emily Campbell, Associate Vice President for Operations and Decision Support, Office of the Executive Vice President and Provost
Terry Johnson, University Chief Financial Officer and Treasurer
Iowa Board of Regents
Office of Auditor of State

BOARD OF REGENTS
Governing Iowa's Public Universities

**Office of Internal Audit**

2nd Floor Warren Madden Building
Ames, Iowa 50011-3603

**IOWA STATE UNIVERSITY**
**AUDIT FOLLOW-UP**
**M E M O R A N D U M**

TO: Cory Harms, Chief Procurement Officer

FROM: Amanda McCoy, Auditor
Joshua Randall, Assistant Audit Director
Chad Sharp, Chief Audit Executive

DATE: April 22, 2026

SUBJECT: Procurement Services

The Procurement Services audit report was issued on November 12, 2025. A follow-up review has been conducted to assess management's progress in implementing corrective actions identified in the original report.

**Recertification Training Expectations** – Cardholder recertification training has been created and implemented. Recertification requirements have been documented and communicated to cardholders.

**Shared Travel and Hospitality Card** – Procurement Services meets with Finance Service Delivery (FSD) bi-weekly to discuss operational issues and areas for improvement. Training has been developed and incorporated into FSD's Continuous Improvement Hours Recurring Training Topics Course Catalog. This training is scheduled to take place in August of each year.

**Payment Timeliness** – Procurement Services meets with FSD bi-weekly to discuss payment-related issues and identify process improvements. Average invoice entry time continues to improve due to utilizing recently implemented invoice intake and processing automation software. Training for Cost Center Managers has been developed and will be released in collaboration with other financial training being developed outside of Procurement Services.

Management has been proactive in addressing each of the original recommendations. The audit is now closed.

cc: David Cook, President
Sean Reeder, Senior Vice President for Operations and Finance
Heather Paris, Associate Vice President for Finance
Stacy Sassman, Associate Director, Procurement Services
Jamie Albertsen, Associate Director, Procurement Services
Iowa Board of Regents
Office of Auditor of State

BOARD OF REGENTS
Governing Iowa's Public Universities

Office of Internal Audit
2nd Floor Warren Madden Building
Ames, Iowa 50011-3603

# IOWA STATE UNIVERSITY
## AUDIT FOLLOW-UP
## M E M O R A N D U M

TO: Charlotte Hampson, Director of Student Wellness, Student Health and Wellness
Erin Baldwin, Associate Vice President, Student Health and Wellness

FROM: Breana Hardman, Auditor
Joshua Randall, Assistant Audit Director
Chad Sharp, Chief Audit Executive

DATE: April 22, 2026

SUBJECT: Student Wellness

The Student Wellness audit report was issued on September 17, 2025. A follow-up review has been conducted to assess management's progress in implementing the corrective actions identified in the original report.

**Program Procedures** – Key processes for Student Wellness programs have been documented. Additionally, onboarding and training procedures for staff have been created.

**Student Wellness Budget** – A budgeting plan has been developed outlining all program dollars to be justified based on demonstrated need, student reach, documented outcomes, and alignment with strategic priorities directing resources flow to the highest-impact services that support student wellbeing. Additionally, Students Helping Our Peers (SHOP) has created and documented a budget structure including the organization and management of all SHOP funding sources.

**Volunteer Training Tracking** – A standard operating procedure (SOP) has been developed for volunteer training. This includes the process for tracking volunteer training to include pre-scheduling confirmation, as well as monthly verification by the program specialist and/or operations manager.

**SHOP Oversight** – SHOP procedures and the student organization affiliation agreement have been updated to reflect current processes. Additionally, a process to review physical access for the SHOP has been implemented to occur each semester.

**Emergency Plan** – An emergency action plan has been established in compliance with the Food Bank of Iowa contract. The emergency action plan has been included in the SHOP SOP document and covers pandemic and equipment malfunction processes.

**Software Management** – Student Wellness has collaborated with the ISU Information Technology Workday Integration unit to implement a verification system so SHOP resources are utilized only by ISU students. Additionally, a user access SOP was created for consistent software access review.

Management has been proactive in addressing each of the original recommendations. The audit is now closed.

cc: David Cook, President
Sean Reeder, Senior Vice President for Operations and Finance
Toyia Younger, Senior Vice President for Student Affairs
Sara Parris, Associate Director for Administrative Services, Thielen Student Health Center
Iowa Board of Regents
Office of Auditor of State

BOARD OF REGENTS
Governing Iowa's Public Universities

Office of Internal Audit
219 Sabin
Cedar Falls, Iowa 50614-0319

**UNIVERSITY OF NORTHERN IOWA**
**AUDIT FOLLOW-UP**
**M E M O R A N D U M**

TO: Maureen Clayton, Associate Dean, College of Humanities, Arts, and Sciences
Mary Black, Dean, College of Humanities, Arts, and Sciences
Jose Herrera, Provost and Executive Vice President

FROM: Amanda McCoy, Auditor
Joshua Randall, Assistant Director
Chad Sharp, Chief Audit Executive

DATE: April 22, 2026

SUBJECT: College of Humanities, Arts, and Sciences

The College of Humanities, Arts, and Sciences audit report was issued on April 23, 2025. A follow-up review has been conducted to assess management's progress in implementing the corrective actions identified in the original report.

**Formalized Expectations** – First year benchmarks were set by department heads, reviewed by the dean, and documented with the Dean's Office. Benchmarks for future years will be provided by the dean to the department heads and retained with the Dean's Office.

**Budgeting Process** – Strategies have been developed and approved to enhance the accuracy of budget creation, reduce deficits, and achieve balanced budgets.

**IT Software Purchasing** – All collegiate employees with procurement cards and travel and hospitality Cards have completed required training.

Management has been proactive in addressing each of the original recommendations. The audit is now closed.

cc: Mark Nook, President
Michael Hager, Senior Vice President for Finance and Operations
Iowa Board of Regents
Office of Auditor of Sta

# STATUS OF AUDIT FOLLOW-UPS

## University of Iowa

| Title | Report Date | Original Follow-Up Date | Revised Follow-Up Date | Action Status |
|---|---|---|---|---|
| 1. Medical Center Downtown Building Security and Access | Feb 27, 2025 | Feb 2026 | Aug 2026 | |
| 2. Department of Anatomy and Cell Biology | Nov 12, 2025 | March 2026 | | |
| 3. Housing and Dining Key Management | Nov 12, 2025 | April 2026 | | |
| 4. Medical Center Downtown Revenue Cycle | Feb 25, 2026 | May 2026 | | |
| 5. StarRez | June 11, 2025 | June 2026 | | |
| 6. Department of Chemistry | Nov 12, 2025 | July 2026 | | |
| 7. Department of Internal Medicine | June 11, 2025 | July 2026 | | |
| 8. Magid Center for Writing | Sept 17, 2025 | July 2026 | | |
| 9. Department of Cinematic Arts and CLAS Production Unit | Feb 25, 2026 | Aug 2026 | | |
| 10. Department of Urology | Feb 25, 2026 | Aug 2026 | | |
| 11. University of Iowa Research Foundation | Feb 25, 2026 | Sept 2026 | | |
| 12. Medical Center Downtown Central Sterilizing | Feb 25, 2026 | Oct 2026 | | |
| 13. UI Health Care Enterprise Scheduling Operations | Feb 25, 2026 | Dec 2026 | | |

## Iowa State University

| Title | Report Date | Original Follow-Up Date | Revised Follow-Up Date | Action Status |
|---|---|---|---|---|
| 14. 4-H Youth Development | Sept 17, 2025 | Jan 2026 | April 2026 | |
| 15. Center for Statistics and Applications in Forensic Evidence | Feb 22, 2026 | May 2026 | | |
| 16. Research and Demonstration Farms | Nov 12, 2025 | May 2026 | | |
| 17. Cash Management and Investments | June 11, 2025 | July 2026 | | |
| 18. Institutional Research | Feb 25, 2026 | Nov 2026 | | |
| 19. Ivy College of Business | Feb 25, 2026 | Dec 2026 | | |

## University of Northern Iowa

| Title | Report Date | Original Follow-Up Date | Revised Follow-Up Date | Action Status |
|---|---|---|---|---|
| 20. Office of Civil Rights Compliance | April 24, 2024 | Jan 2025 | June 2026 | |

## Follow-Up Legend

| | |
|---|---|
|  | • Planned corrective action and/or follow-up report not completed within six months of originally scheduled date. |
|  | • Planned corrective action and/or follow-up report not completed within three months of originally scheduled date. |
|  | • Follow-up report is due and is within three months of originally scheduled completion date. |
|  | • Follow-up report not yet due. |