University of Sydney report on implementation of plan of action in response to *Investigation into the over-payment of public funds by the University of Sydney for security services* (Operation Gerda)

Please indicate which applies:

- ❑ **This is a final report; the plan of action is fully implemented**

As previously advised, the scope and scale of recommendations made in investigation reports varies considerably, as do the plans of action public authorities develop in response.

The Commission recognises a single template may not be effective for reporting on the implementation of all action plans. In view of this, the University of Sydney is invited to use a reporting format that best illustrates the comprehensiveness of the implementation of the plan of action.

The Commission asks that proposed report formats are discussed with the ICAC's corruption prevention representative named in the cover letter. The ICAC corruption prevention representative will advise if the report format has the Commission's endorsement.

However, if the University of Sydney prefers to adhere to an established format, the following may be used as a guide.

Report (final)

Recommendation 1

That the University ensures that key tender documentation, such as procurement strategies, tender evaluation plans and tender evaluation committee (TEC) reports, include a realistic and detailed assessment of procurement and contract risks. This assessment should be conducted in a manner that incorporates operational risks and complies with the risk management principles in the International Standard on Risk Management ISO 31000:2018.
Status: Implemented **Background:** The University has adopted a tiered approach to assessment and documentation requirements when purchasing goods or services, based on the value of the purchase. The degree of diligence required increases as the cost of the purchase increases. Preferred suppliers The University has a range of preferred suppliers who have been appointed through a University Procurement Services-led competitive process, such as an open Request for Tender. Each preferred supplier is subject to a master contract agreement detailing the terms and conditions of supply.

Wherever possible, University staff are encouraged to place orders for goods and services through one of the University's preferred suppliers. Where University staff choose not to use the University's preferred supplier the purchase is automatically directed to the UniBuy Desk (procurement help desk) who assist with buying low value goods and services and assess and document reasons for choosing a non-preferred supplier. The UniBuy Desk can also recommend the use of an alternative supplier.

Quotation or tendering process

Where the University does not have a preferred supplier, University staff obtain quotes or follow a tendering process, applying the thresholds noted below:

Value of goods/services (excl GST)	*Requirement/channel*
Less than $5,000	Corporate card, if infrequent and not available from a UniBuy catalogue established with contracted suppliers
$0 to $29,999 (Simple buying)	Obtain at least **one** written quote
$30,000 to $249,999 (Comprehensive buying)	Obtain at least **three** written quotes
$250,000 and above (Tailored sourcing)	Must go through a tailored tendering process

This background is relevant to Recommendations 1; 2; 3; 4; 5; 6; 7; 8; 9; and 10. These recommendations all relate to ***tender*** processes (which may include a Request for Quote, Request for Proposal, Request for Tender or a multi-stage event). As outlined above, the University uses tender processes to establish contracts with preferred suppliers for the purchase of goods or services with a value of $250,000 or more (excluding GST). The University's responses to Recommendations 1 to 10 relate to the documentation and assessments used in its tender processes.

Action Taken: For all tender processes, the University uses a range of key document templates provided to sourcing specialists (Procurement Services specialists who manage procurement projects with a total contract value over $250,000 (exclusive of GST)), designed to address the University's key risks. The listing below outlines these documents, following the process-flow of a typical tender:

- **Risk Evaluation Framework** to assess the risks to be addressed during the tender process
- **Procurement Strategy**, supported by External Interest Declarations and Confirmation of Funding
- **Probity Questionnaire** to assist in assessing whether a Probity Adviser is required and to document the final decision
- **Complexity Matrix** to assist in assessing whether the Request for Tender and the Tender Evaluation Plan should be referred to the Chief Procurement Officer, for review and approval
- **Request for Tender** with generic and project-specific questions covering risk areas for all projects, for example, sub-contracting and ethical practice. This document also includes the University's **Conditions of Tendering**

- **Tender Evaluation Plan**. This document establishes evaluation criteria and weightings and includes **Scoring Guidelines**
- **Tender Evaluation Charter**. This document includes matters relating to the management of evaluations.
- **Tender Evaluation Report** which details the outcome of the evaluation process and recommends the award
- **Approval to Award** which outlines the procurement process and the outcome of the evaluation for approval under established governance and the University's Delegations of Authority (where approval is not required from the Finance and Audit Committee)
- **Finance and Audit Committee Paper**, (via the University Executive) where required by the University's Delegations of Authority.

The University completed an update of its procurement templates in December 2020 to ensure that key tender documentation, such as the Procurement Strategy, Tender Evaluation Plan and Tender Evaluation Report, require staff running the tender process and business stakeholders to include a realistic and detailed assessment of procurement and contract risks. Risk is reviewed by approvers at the Procurement Strategy and Approval to Award stages of the procurement project and for high risk or high value projects risk, is also reviewed at Request for Tender and Tender Evaluation Plan stages.

The Risk Evaluation Framework template has been designed to ensure that the assessment of procurement and contract risks by the staff running the tenders will include operational risks. For instance, the Risk Evaluation Framework prompts consideration of the risk of supplier or sub-contractor fraud. The Risk Evaluation Framework template has been developed in collaboration with the University's Chief Risk Officer and is aligned with the University's Risk Management Framework and Risk Appetite and Tolerance Statement which comply with the risk management principles in the International Standard on Risk Management ISO 31000:2018. The Risk Evaluation Framework was implemented in late 2019 and made a mandatory step in the tendering process with effect from January 2020 following training for the procurement team members.

All guidance and training material is stored in the procurement Knowledge Library and is available for all team members. An onboarding training program has been developed for new starters which will be mandatory from Q3 2021.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 2

That the University amends its *Guidelines for using the risk assessment tool* to provide more detailed guidance on major contract risks.

Status: Implemented

Background: Please refer to the Background outlined in Recommendation 1.

Response: As part of the key documents outlined in the response to Recommendation 1, the University requires staff running tender processes to complete a Risk Evaluation Framework document to ensure that major contract risks are considered and assessed. The Risk Evaluation Framework, supported by Risk Assessment Guidelines (replacing the Guidelines for using the risk assessment tool), was updated in October 2019 to provide more detailed guidance on major contract risks, by providing guidance on mitigating major risks and prompting appropriate mitigations, together with training for the procurement team facilitated by Office of General Counsel and the Chief Risk Officer. Ongoing training will be provided to the procurement team to maintain the quality of risk assessments as a key part of the sourcing process.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 3

That the University assesses contract assurance frameworks that cover key risks involved in the provision of services, such as a reliance on subcontracting, when assessing the capability and capacity of tenderers.

Status: Implemented

Background: Please refer to the Background outlined in Recommendation 1.

Response: As outlined in the response to Recommendation 1, the University's sourcing specialists use a suite of document templates designed to address key risks to the University in relation to risks involved in procurement of services. Tenderers are required to agree to an appropriate contract assurance framework that covers these key risks involved and a reliance on subcontracting is expressly identified when relevant. These key risks are initially captured when the Risk Evaluation Framework is completed.

Relevant key documents used by the University to assess the capability and capacity of tenderers in addressing these key risks include the:

- Risk Evaluation Framework which identifies and assesses risks to be addressed during the sourcing process.
- Request for Tender, which includes both generic and project-specific questions covering risk areas for all projects, including sub-contracting and ethical practice.
- Tender Evaluation Report, which includes assessments of the contract assurance frameworks outlined by tenderers in their submissions.

University contract templates have also been enhanced to reflect risk areas including ethical practice and sub-contracting. The University’s standard contract templates mandate that suppliers seek approval from the University before appointing a sub-contractor and the primary supplier is responsible for the actions and performance of its sub-contractors.

The University also has in place a Contract Management Framework which provides guidance for contract managers on how to manage risks during the course of the contract - and in the tiering of contracts on the basis of risk to determine the level of management required.

Contract tiering occurs towards the end of the sourcing activity, when sourcing staff and the contract owner within the business unit will establish a contract ‘risk’ review that will ultimately determine how the contract will be managed post award. This commenced from June 2021 and will continue to be refined.

In addition, contract managers across the University Operations portfolio have attended mandatory contract management training conducted by a company called Informa and delivered by one of their agents qualified in contract law. An online training course is currently in development. Once complete, it will form part of the mandatory induction training for new Contract Managers through the University's Learning & Development platform and will also be available for ongoing reference as needed

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 4

That the chief procurement officer formally reviews requests for tender (RFTs) for high-risk tenders and tender evaluation plans for significant procurement undertakings.

Status: Implemented

Background: Please refer to the Background outlined in Recommendation 1.

Response: A complexity matrix, introduced in August 2020, determines the complexity of the tender by reference to the level of risk and dollar value of a procurement request.

If the outcome of the complexity matrix assessment indicates that the tender has a high risk or high value (requiring financial approval by the Finance and Audit Committee – over $10M (exclusive of GST)), the Request for Tender and the Tender Evaluation Plan documentation is submitted to the Chief Procurement Officer for formal review and approval.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 5

That the University should review its tender assessment criteria and weightings to avoid perceptions that unwarranted advantages are provided to a particular tenderer.

Status: Implemented

Background: Please refer to the Background outlined in Recommendation 1.

Response: As outlined in the response to Recommendation 1, the University uses a range of key document templates in tender processes which are designed to identify and address the University's key risks.

The University's Risk Evaluation Framework (which prompts key risks requires a project by project assessment of likelihood and consequence)has been updated to specifically flag the risk of incumbent advantage and, in addition, training has been provided by the Office of General Counsel highlighting the need to maintain fairness in the tendering process through, for example, non-product specific requirements and disclosure of all relevant information to all tenderers, so that staff involved in the tender process can ensure that tender assessment criteria and weightings avoid the perception that unwarranted advantages are provided to a particular tenderer.

Tender Evaluation Committees are comprised of individuals with the most comprehensive knowledge of the goods and services being sourced. This may mean that a contract manager is included on the team, subject to disclosing conflicts of interest and, where required, entering into a Conflict Management Plan. An element of the procurement lead's role is managing the probity and fairness of the procurement process, including undue influence brought to bear on Committee members.

This is complemented by:

- The Procurement Strategy, which has been updated to require high level risks and tender evaluation criteria to be identified
- The Probity Questionnaire, which includes specific consideration of whether the risk or circumstances involved in the tender require the appointment of an independent Probity Adviser to avoid any perception of bias or favouritism
- Guidance notes on managing favouritism and bias.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 6

That probity walls and/or other safeguards should be established where there is a risk that someone connected to a tenderer could access confidential information about a tender process and tenderers' submissions.

Status: Implemented

Background: Please refer to the Background outlined in Recommendation 1.

Response: The University has a range of processes to identify whether staff or contractors involved in a tender process could have a conflict of interest, such as being connected to a tenderer, so that appropriate measures such as probity walls and/or other safeguards can be put in place to ensure that they cannot access confidential information about the tender process and/or the tenderers' submissions.

At an overarching level, the University's Procurement Policy requires every person undertaking procurement activities to behave ethically and to monitor, report and manage any actual, apparent or perceived conflicts of interests. This requirement is complemented by the University's External Interests Policy.

At an individual tender level, the Procurement Strategy document requires completion of External Interest Declarations flagging any actual, apparent or perceived conflicts of interest. This is complemented by the Tender Evaluation Charter, which highlights the need to disclose conflicts of interest and must be formally acknowledged by all the members of the Tender Evaluation Committee.

The University's tender processes are supported by procurement personnel whose training includes awareness of the need to ensure that probity walls and/or other safeguards are put in place where there is a risk that someone connected to a tenderer could access confidential information about a tender process and tenderers' submissions. Where actual, perceived or potential conflicts of interest are identified, the individuals involved are either excluded from the tender process or an appropriate Conflict Management Plan is prepared and monitored by the procurement lead.

Conflict Management Plans can address conflicts of interest by removing conflicted persons from the tender process, restricting the conflicted person’s involvement in stages of the procurement process or ensuring that the conflicted person is involved in group decision-making rather than making decisions or influencing outcomes alone.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 7

That the University should ensure consistency across its tender documentation concerning how tenders will be evaluated.

Status: Implemented

Background: Please refer to the Background outlined in Recommendation 1.

Response: As outlined in the response to Recommendation 1, the University uses a range of key document templates, which are provided to procurement personnel for use in tender processes, designed to address the University’s key risks. The University has reviewed and updated these document templates to ensure consistency across its tender documentation concerning how tenders will be evaluated. Relevant documents which have been updated include the:

- Request for Tender, incorporating The Conditions of Tendering, reviewed in June 2020
- Tender Evaluation Plan, including Scoring Guidelines, reviewed in November 2019
- Tender Evaluation Charter, including matters relating to the management of evaluations, reviewed in November 2019.

In particular, the Tender Evaluation Charter establishes a consistent approach to the evaluation of tenders, providing guidance on:

- Principles of an evaluation
- Management of the tender evaluation
- Arrangements to ensure confidentiality, fairness and probity
- Roles and responsibilities of Tender Evaluation Committee members
- Tender evaluation criteria – guidance around types of criteria, setting and evaluating
- The evaluation process and methodology – steps in the process, management of late and alternative tenders
- Recommendation and approval – how the recommendation of the Committee is taken forward for approval
- Notifications and contract negotiations – the appropriate time to notify tenderers of the outcome, finalising contract matters and debriefing unsuccessful respondents.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 8

That the University should continue to assess all tenderers and, where relevant, their supply chains to ensure compliance with Awards.

Status: Implemented

Background: Please refer to the Background outlined in Recommendation 1.

Response: As outlined in the response to Recommendation 1, the University uses a range of key document templates provided to sourcing specialists in tender processes, designed to address the University's key risks. This includes the risk that all tenderers and, where relevant, their supply chains ensure compliance with Awards. Relevant key documents include the:

- Risk Evaluation Framework identifying compliance with Awards as a risk where appropriate.
- Request for Tender with generic and project-specific questions covering risk areas for all projects including sub-contracting and ethical practice including, but not limited to, acknowledging the University's Statement of Business Ethics, disclosing involvement in any investigation or prosecution for any fraud or misconduct or any allegations of wage theft or similar.

There are also specific requests for information regarding relevant Industrial Awards and the tenderer's history in complying with those Awards including but not limited a confirmation that the tenderer has processes and systems in place for ensuring wages are paid to staff in accordance with applicable laws and agreements:

- Tender Evaluation Plan which highlights the approach taken during the procurement process to review the tenderer's submitted rates in labour-based contracts against relevant Industrial Awards.
- Tender Evaluation Report outlining the University's assessment of the submissions and representations made by the tenderers.

In addition, training has been provided to the procurement team to enable them to identify circumstances in which labour-based services require validation against awards and processes and approaches to use to carry out this validation.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 9

That all TEC chairs and/or appointed probity advisers should ensure that tender scoring methodologies are clear to evaluators and that the tender assessment criteria have been followed.

Status: Implemented

Background: Please refer to the Background outlined in Recommendation 1.

Response: Each Tender Evaluation Committee (TEC) is assisted by procurement personnel, with training in tender processes and awareness of the need to ensure that the tender scoring methodologies are clear to evaluators and that the tender assessment criteria have been followed. In the case of very complex or sensitive tenders, the procurement lead may be supported by an independent probity adviser engaged by the University.

As outlined in the response to Recommendation 1, the University uses a range of key document templates provided to sourcing specialists in tender processes, designed to address the University's key risks.
Relevant documents include the:

- Tender Evaluation Plan which includes evaluation criteria and weightings and Scoring Guidelines
- Tender Evaluation Charter which includes guidance around the tender evaluation criteria and the evaluation process and methodology. All members of the Tender Evaluation Committee must formally acknowledge this Charter.
- Tender Evaluation Report.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 10

That tender reports to the Finance and Audit Committee (FAC) and the tender board should contain adequate information to enable key issues to be understood. The information should include:

- **tenders' assessment criteria scores**
- **key contract risks and their mitigation**
- **key assumptions**
- **any significant probity concerns and the manner in which they were resolved.**

Status: Implemented

Background: Please refer to the Background outlined in Recommendation 1.

Response: Once the tender process has been conducted and the Tender Evaluation Report has been produced, the recommendations are documented in the Approval to Award and submitted to the University's Tender Board for review and approval. The Approval to Award summarises the procurement process, evaluation outcomes (including scores for each tenderer) and identifies residual risks for handover to the Contract Manager. For high-value contracts which require approval by the University's Finance and Audit Committee under the University's Delegations of Authority, a submission is prepared for approval.

The content of reports to the Finance and Audit Committee has been enhanced to ensure it is comprehensive and contains adequate information to enable key issues to be understood, including:

- A summary of the procurement process including the stages of the process (e.g. Expression of Interest or Request for Information followed by a Request for Tender and tenderer assessment at each stage)
- Scores for each tenderer against pre-determined criteria and weightings
- Key procurement and contract risks and their mitigation as well as residual risks to be managed by the Contract Management
- Key assumptions leading to decisions and recommendations.
- Any significant probity concerns and the manner in which they were resolved.

Precedent papers have been made available to procurement team on which to base submissions and guidelines have been published to assist the team in drafting submissions.

Approvals to Award presented to the Tender Board are reviewed and approved by business owners and the procurement team, including the Chief Procurement Officer. In the case of submissions to the Finance and Audit Committee, there is a comprehensive review of papers prior to presentation by the Associate Director – Commercial Strategy Team, the Associate Director – Quality, Governance and Performance and the Chief Procurement Officer. Submissions to the Finance and Audit Committee are also reviewed by the Chief Financial Officer.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 11

That the University should ensure all future contracts for the provision of security services include adequate provisions covering:

- **subcontracting terms**
- **contractor assurance frameworks**
- **right-to-audit clauses**
- **timesheet access**
- **technology requirements.**

Status: Implemented

Background: Since the ICAC Operation Gerda investigation and public hearing, the University's Campus Infrastructure Services (CIS) portfolio has been split into two professional service units:

- University Infrastructure (UI), responsible for planning and design, property development, infrastructure delivery, space and sustainability
- Central Operations Services (COS), responsible for Asset management, maintenance services and operational services (I.e. repairs, cleaning, internal mail, waste collection and recycling, security services, building access, venue bookings etc.)

Response: In 2019, the University executed a new main contract "Operations Services Agreement" for the provision of security services, which covers the main volume of services performed.

Note: There are also two small (Less than $30k p.a.) agreements for security services also in place for remote locations, which have applied management controls. These controls are applied in proportion to the small volume of services performed, under these Agreements.

The main contract includes provisions covering:

- Subcontracting terms – the contractor must not subcontract any part of the services without first obtaining the University's prior written approval of the services to be subcontracted and of the proposed subcontractor.
- Contractor assurance frameworks – the contractor must maintain an administration manual covering aspects such as quality assurance, work health and safety policy, risk management and risk register, requirements of the modern Award, and an audit and inspection plan developed in accordance with the contractor's quality assurance framework.
- Right-to-audit clauses – the University has rights to audit the contractor's records to verify compliance with the contract.

- Timesheet access – the daily physical timesheets of contractor staff are held by the University's Operations Manager and verified against biometric data confirming the identity of the individuals and the duration of their shift, with follow-up of any variances.
- Technology requirements – the contractor must use the University's Archibus work management system to manage all requirements of the services performed under the contract. Contractor staff must provide biometric data when they commence and scan in and out for individual shifts, to allow verification of timesheet data. Compliance is reviewed monthly, as part of the contractor's key performance indicators under the Operations services Agreement.

The University will ensure that future contracts for the provision of security services include similar provisions.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 12

That security contractors should be required to provide evidence that they have properly implemented internal controls to ensure that security staff (including subcontractors) have completed their duties in accordance with the contract and work orders.

Status: Implemented

Response: The University's new contract for the provision of security services imposes this obligation on the contractor.

At a framework level

Under the new Operations Services Agreement, the contractor is required to maintain a performance management framework and quality assurance plan. This is supported by detailed reporting requirements around work management, compliance, and key performance indicators. The University also has right-to-audit access to the contractor's records.

At a granular level

Under the Operations Services Agreement, contractor staff must provide biometric data when they commence and scan in and out for individual shifts, to allow verification of timesheet data, and complete physical timesheets. Compliance with these obligations is formally reviewed monthly as part of the contractor's key performance indicators. If any performance issues are identified they are addressed within the monthly performance review meetings. Depending on severity of the non-compliance a Corrective Action Requirement (CAR) or Breach would be raised, as per the contractual conditions.

The daily physical timesheets of contractor staff are held by the University's Operations Manager and verified against the biometric data confirming the identity of the individuals and the duration of their shift, with appropriate follow-up of any variances.

At month end, the University reviews the contractor invoices submitted against the contract and any work orders, and reconciles the verified timesheet data against the contractor invoices, to evidence that the security staff (including subcontractors) have completed their duties in accordance with the contract and work orders.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 13

That the University should document its internal contractor controls. A report of the conduct of the controls, exceptions to the controls and the resolution of those exceptions should be given to relevant managers in CIS.

Status: Implemented

Background: As outlined in the Background to Recommendation 11, CIS has now been split into two professional service units, University Infrastructure (UI) and Central Operations Services (COS).
Response: Informed by the recommendations of Operation Gerda, the University undertook a careful review of its internal contractor controls in relation to security, the conduct of the controls and deficiencies in historical control measures. The tender specifications for the Operations Services Agreement for the provision of security services was developed to ensure that it resolved any deficiencies and implemented a robust framework for implementing and monitoring key internal contractor controls, including:

- Contract Management Plan – Outlines the requirements and governance to manage the contract (s) requirements.
- Contract Guide – Provides the key drivers and obligations to meet minimum deliverables and maximise opportunity.
- Contract Deliverables – Provides a listing with key accountability of each of the deliverables for both parties.
- Contractor Administration Manual – Provides full transparency of what, when and how the contractor is required to meet the contractual requirements, set within the Agreement.
- Key performance indicators and reporting - Outlines the performance expectations to regulate and effectively manage performance obligations.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 14

That the University should perform random checks that security guards are on duty. These could include GPS monitoring, reviewing CCTV and access records, and surprise visits to certain locations.

Status: Implemented

Response: Subject to compliance with privacy requirements, the University undertakes random checks to ensure that security guards under the main contract are on duty on a 24 hours a day, 7 days a week basis. Checks are undertaken by the University's Operations Controllers using a variety of methods:

- Review of rosters and biometric scan in and scan off data
- Review of CCTV footage
- Surprise visits to locations to verify presence.

A record of these checks is maintained as part of "end of shift" reporting requirements and is submitted on a daily basis to the Head of Security and Emergency Management and the Director Asset Management and Operations for independent review. The information is also available for cross-checking purposes when the month-end invoice checks are undertaken. Compliance is tracked and formally reported through the monthly contractor key performance indicators process.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 15

That there should be a regular rotation between at least two University employees who undertake contractor checks to ensure that security services are provided.

Status: Implemented

Response: As outlined in the response to Recommendation 14, random checks on security guards are undertaken by the University's Operations Controllers. The Operations Controller position is covered by two people on a 24-hours a day, 7 days a week basis, overseeing all contracted labour and providing verification that security services were provided. A record of these checks is maintained as part of "end of shift" reporting requirements and is submitted daily to the Head of Security and Emergency Management and the Director Asset Management and Operations for independent review.

Ongoing internal audits and compliance reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 16

That the University should have access to guard timesheets. The University should also inspect the timesheets to ensure compliance with legislative requirements and the contract, and to help confirm charges on invoices.

Status: Implemented

Response: Under the University's new main contract for the provision of security services, the daily physical timesheets of contractor staff are held by the University's Operations Manager and verified against biometric data confirming the identity of the individuals and the duration of their shift, with appropriate follow-up of any variances.

The University inspects the timesheets to ensure compliance with legislative requirements and the contract.

At month end, the University reviews the contractor invoices submitted against the contract and any work orders, and reconciles the verified timesheet data against the contractor invoices, to evidence that the security staff (including subcontractors) have completed their duties in accordance with the contract and work orders and to confirm the charges on the invoices.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 17

That security contractors should be required to provide specimen signatures against which the signatures of guards should be checked.

Status: Implemented

Response: Under the University's new main contract for the provision of security services, when contractor staff commence, they must attend a University induction and produce their Driver's Licence or NSW Photo Card, which includes a specimen signature contained within their licence/card. The University retains a copy of the signature on a secure electronic portal as a reference. At the induction, the contractor staff provide biometric data which defines the security staff identification profile, which provides identity verification when they scan in and scan off at the start and end of shifts. The biometric compliance is measured daily and measurable under the KRA / KPI monthly contractual obligation. The Biometric fingerprint is one of the verifications used by the university for payment of invoices under the Operations Services Agreement

These identity requirements (signature, Biometric, etc) must be verified for any security staff to undertake any duties.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 18

That the University should have key performance indicators (KPIs) in place that cover the essential requirements for the provision of security services. It should also ensure KPI monitoring for security contracts is based on data that is trustworthy, measurable and relevant, and that reliance on contractor self-reporting is minimalised.

Status: Implemented

Response: Under the University's new main contract for the provision of security services, the University has established key performance indicators (KPIs) that cover the essential requirements for the provision of security services. Key clauses and schedules, within the contract, which outlines the KPI requirements include:

- Performance management framework (clause 12 and Schedule 5)
- Reporting requirements (Schedule 4)
- Security Services key performance indicators (Schedule 7).

The contractor's KPI performance is reviewed and monitored by the University:

- On a monthly basis via formal contract performance reporting and engagement.
- On a quarterly basis via discussion in a steering committee with Contract Senior Management
- On an annual basis via a formal contract review.

To ensure that the KPI monitoring for security contracts is based on data that is trustworthy, measurable and relevant, and that reliance on contractor self-reporting is minimised, the University sources or independently verifies the KPI data via the University's Central Operations Services Service Excellence and Innovation team.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 19

That the University should develop controls to identify when contract variations exceed 10% of the original contract amount. It should also clarify that a sufficiently senior delegate is required to scrutinise and approve cumulative ad hoc contract payments that exceed 10% of the contract value.

Status: Implemented

Response: The current Operations Services Agreement total contract value is endorsed by Financial Advisory Committee (FAC). Any variation regardless of the value are quantified and verified by the principal's representative. The FAC approved contract value cannot be exceeded unless FAC and Vice Chancellor endorsed under the set University Delegations of Authority.

All ad-hoc requests issued, regardless of value, have an individual service request by the university, before they are issued to the Security contractor to perform the works. Multi-level verification is undertaken for all ad-hoc payments against the claimed amount, which is verified and checked by senior management at each billing period.

All contracts sourced by Strategic Procurement and loaded into the UniBuy system have control mechanisms that do not allow for overspend without appropriate approval by staff with appropriate delegations of authority. A contract with a value over $250,000, excluding GST, is executed the approved estimated or fixed value is entered into the system. When purchase orders are raised against the contract they are accumulated and deducted from the approved value. The approved value has been exceeded the Contract is automatically closed and no further spend is permitted. To re-open the contract a variation must be approved by the appropriate financial delegate for the total accumulated value of the contract. No deviations are permitted under the delegations of authority.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 20

That the University considers sharing some contract management duties between internal staff, who are co-located with security contractors, and staff, who do not have day-to-day contact with security contractors.

Status: Implemented

Response: Under the University's new Operations Services Agreement, the University has introduced appropriate separation and segregation of duties between University and contractor staff.

The security contractor has been provided with an office location in a separate building from the University's security staff and the University's contract management staff, so there is no co-location.

The work of the security contractor staff is supervised by University Operations Controllers. The Operations Controller position is covered by two University staff on a 24-hours a day, 7 days a week basis, overseeing all contracted labour and providing verification that security services were provided.

The Operations Controllers are supervised by the University's Security Operations Manager and the Head of Security and Emergency Management, who reports to the Director Asset Management and Operations.

Contract management data verified and provided by the Operations Controllers, the Security Operations Manager and the Head of Security and Emergency Management is submitted to the Central Operations Services Service Excellence and Innovation team for review and confirmation of correlation to information submitted by the contractor. The head of the Service Excellence and Innovation team has a direct reporting line to the Executive Director Central Operations Services, independent from the Director Asset Management and Operations who is responsible for the security services team.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 21

That the University should develop a code of business practice or similar document and contractually bind major suppliers to comply with it. The document should include:

- **a prohibition on suppliers or potential suppliers offering gifts and benefits**
- **a prohibition on actions that place University staff or other individuals in the supply chain in conflict of interest situations**
- **a requirement for suppliers to have comparable provisions in contracts with subcontractors or other companies in the supply chain**
- **details of where people can make reports (including anonymous reports) of breaches of the code of business practice.**

Status: Implemented

Response: The University has developed and published a Statement of Business Ethics which states the University expects where organisations and business operators carry out work on behalf of the University they will:

- Not offer financial inducements, gifts or benefits to University employees, contractors and consultants which might directly or indirectly compromise, influence, or appear to influence them in their official University capacity
- Disclose any actual or perceived conflicts of interest and report any unethical behaviour immediately
- Act ethically always and conduct themselves in a professional, fair, and constructive manner in all their dealings with the University
- Report unethical practice, misconduct, fraud, or corruption as soon as they become aware of it.

The Statement of Business Ethics includes a link to the University's Reporting Wrongdoing Policy which details how people can make reports (including anonymous reports) of breaches. Entering in the word "wrongdoing" on the University's home webpage search tool returns the Report wrongdoing webpage, which provides information on wrongdoing including a link to the University's anonymous online reporting facility.

The University's Request for Tender template document has been updated to include a link to the Statement of Business Ethics and to require tenderers to confirm that they will comply with its requirements. This is mirrored in the University's standard contract templates, which have been updated to require suppliers to comply with the Statement of Business Ethics and, in addition, to require the supplier ensures any subcontractors comply with the terms of the contract.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 22

That the University should establish a clear mechanism, and one that is clearly communicated, for the staff of suppliers and subcontractors to report corrupt conduct.

Status: Implemented

Response: The University has updated its:

- Statement of Business Ethics to include a direct reference to the University's Report wrongdoing webpage, and to require suppliers to notify their representatives of the webpage
- Standard procurement contract templates to require suppliers to notify their representatives of the Statement of Business Ethics and the Report wrongdoing webpage.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 23

That the University adopts a fraud and corruption control plan that appropriately addresses the risks of fraud and corruption. Among other things, the plan should reflect the findings made in previous Commission investigation reports concerning universities and ensure that the corruption prevention issues are not dealt with in isolation, but that the cumulative implications are properly considered.

Status: Implemented

Response: The University has researched and developed a Fraud and Corruption Control Plan (Plan) tailored to its circumstances. The Plan is based on the concepts outlined in Australian Standard *AS 8001-2003 Fraud and corruption control* and follows its suggested framework structure:

- Executive summary defining concepts and stating the University's attitude to fraud and corruption
- Planning and resourcing
- Fraud and corruption prevention
- Fraud and corruption detection
- Responding to detected fraud and corruption incidents.

The Plan also borrows heavily from the Audit Office of New South Wales *Fraud Control Improvement Kit February 2015* guidelines, as well as being informed by review of fraud and corruption prevention policies and procedures in place at a range of other tertiary institutions.

The fraud and corruption control plan has been submitted to senior University management and has been endorsed by the University Executive (on 8 July 2021) and the Risk and Audit Committee (on 23 July 2021).

The Plan will be published on the Internal Audit website and used to inform future work in fraud and corruption prevention and control across the University.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.

Recommendation 24

That all internal audit reports should be given to the director of internal audit and reported to the FAC. The internal audits should be reviewed by an internal audit manager to assess the implications of the report and whether there are red flags of possible fraud and corruption. If necessary, internal auditors' working papers should also be obtained.

Status: Implemented

Note: During the 2020 calendar year, the University reviewed the structure, responsibilities and terms of reference of its various governance committees. As part of that review, the Finance and Audit Committee was reformed as the Finance Committee and a new Risk and Audit Committee was established. As a consequence of these changes, from 1 October 2020, Internal Audit's reporting line shifted from the previous Finance and Audit Committee (FAC) to the Risk and Audit Committee (RAC). This change in reporting line is reflected in the response below.

Response: Internal Audit has developed a Paper defining what is meant by internal audit reports and outlining the process for advising Internal Audit of locally commissioned internal audit reports. The paper has been approved by the Finance and Audit Committee (on 9 September 2020) and the process was trialled before the paper was submitted to the University's Senior Executive Team and approved by the University Executive (on 18 March 2021). On an ongoing basis, Internal Audit is socialising the paper with senior and local managers to ensure that local areas are aware of the reporting requirement.

When received by Internal Audit, the locally commissioned internal audit reports are reviewed by a Senior Principal Auditor to assess the implications of the report and whether there are red flags of possible fraud and corruption. If necessary, Internal Audit obtains the working papers supporting the locally commissioned internal audit report.

Internal Audit submits an Internal Audit Report to each Risk and Audit Committee meeting. On an as-needed basis, this Internal Audit Report:

- Lists the locally commissioned internal audit reports received and triaged in the period
- Notes which local areas commissioned them
- Summarises Internal Audit's assessment of each report for its implications and any red flags of possible fraud or corruption
- Indicates that the individual reports will be made available to the Committee on request.

Ongoing internal reviews will assess the effectiveness of the actions taken in support of the recommendation.