

POLICY FOR SECURITY AGAINST ECONOMIC CRIME

GOVERNANCE DOCUMENTATION | APRIL 2026



UNIVERSITY OF
SURREY

Contents

STATEMENT FROM THE CHAIR OF COUNCIL	2
PURPOSE AND OBJECTIVE	3
REGULATORY CONTEXT	3
SCOPE AND APPLICATION	3
DEFINITIONS OF KEY TERMS	3
ROLES AND RESPONSIBILITIES	4
MANDATED SYSTEMS AND CONTROLS (RULES)	5
Financial Controls	5
Procurement Controls	6
Human Resource Controls.....	6
Information Systems Controls	7
Research and Innovation Controls	7
Advancement Controls.....	8
Agent Controls.....	9
Student Admissions and Admin Controls	9
Student Finance Controls	10
Disclosure and Reporting Controls	10
Governance Controls.....	10
Monitoring, Metrics, and Assurance	11
Related Documents	11
Document Control	12

STATEMENT FROM THE CHAIR OF COUNCIL

Commitment Affirmation

As senior leaders of the University, we reaffirm our commitment to the highest standards of ethical conduct and to ensuring that all University activities reflect our values, governance expectations, and defined risk appetite. Ethical behaviour is fundamental to our charitable mission, and all staff, contractors, partners, and representatives are expected to uphold these standards consistently.

Zero Tolerance for Economic Crime

The University maintains a zero-tolerance (risk averse) approach to economic crime. Our commitment to this principle is absolute and not contingent on commercial outcome. Protecting the integrity of the institution and the wider academic community takes precedence over any immediate benefit.

Importance for Higher Education

Strong economic-crime prevention safeguards:

- Institutional reputation as a trusted and accountable public body
- Confidence among students, staff, funders, and partners
- Responsible stewardship of public funds, tuition income, research grants, commercial income and philanthropic gifts

These commitments support the University's long-term mission, academic credibility, and public trust.

Endorsement of Policies

We formally endorse the University's Economic Crime Prevention Policy and associated control standards. These documents set out required behaviours, controls, reporting routes, and investigation processes. Compliance is mandatory for all staff and associated persons.

Roles and Responsibilities

Preventing economic crime is a shared responsibility across the institution:

- Vice-Chancellor and Executive Board – overall accountability and oversight
- Chief Financial Officer and Finance Directorate – financial controls and stewardship
- Risk & Compliance – policy development, training, and assurance
- Internal Audit – independent evaluation of control effectiveness
- All staff and associated persons – adherence to policy and prompt reporting of concerns.

Consequences of Breaches

Breaches of the Economic Crime Prevention Policy may result in disciplinary action, contract termination, recovery of losses, or referral to law-enforcement or regulatory bodies, supported by relevant contractual provisions.

Sector Collaboration

The University participates in sector-wide and regulatory initiatives to share intelligence, adopt best practice, and strengthen fraud-prevention efforts across UK higher education.



Charlie Geffen
Chair of Council

PURPOSE AND OBJECTIVE

This policy sets out the Council's expectations regarding system and control arrangements to fulfil its commitment to uphold a zero-tolerance stance on economic crime. It requires the implementation of "reasonable systems and controls" to prevent fraud and other forms of economic crime by individuals associated with the University. By doing so, it evidences ethical conduct and ensures compliance with the Economic Crime and Corporate Transparency Act, as well as relevant legislation and regulations.

REGULATORY CONTEXT

This policy outlines the arrangements to ensure compliance with:

- The Economic Crime and Corporate Transparency Act 2023, including provisions relating to senior manager attribution and the failure to prevent fraud offence.
- The Sanctions and Anti-Money Laundering Act 2018
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
- The Bribery Act 2010
- The Criminal Finances Act 2017
- The Fraud Act 2006 and related offences under the Theft Act 1968
- The Proceeds of Crime Act 2002
- The Public Interest Disclosure Act 1998
- The University also has regard to applicable governance requirements under the Charities Act 2011 and, where relevant, the Companies Act 2006

Compliance is enforced by:

- National Crime Agency (NCA): Responsible for oversight of the Suspicious Activity Reports (SARs) regime and leading investigations into serious and complex economic crime.
- HM Revenue & Customs (HMRC): Enforcement of anti-money laundering supervision (where applicable), tax compliance, and offences relating to the facilitation of tax evasion under the Criminal Finances Act 2017.

- Companies House: Responsible for maintaining the UK companies register and implementing enhanced corporate transparency and identity verification requirements under the Economic Crime and Corporate Transparency Act 2023.
- Office of Financial Sanctions Implementation (OFSI): Part of HM Treasury, responsible for implementing and enforcing UK financial sanctions, including issuing guidance and monetary penalties for breaches.

SCOPE AND APPLICATION

This Policy applies to all individuals and entities acting for, or on behalf of, the University and its subsidiaries, including:

- Employees and officeholders: All permanent, fixed-term, and casual staff, as well as senior managers, directors, and other officeholders.
- Students acting in an official capacity: Including, but not limited to, student ambassadors, paid researchers, and others undertaking activities on behalf of the University.
- Associated persons: Contractors, consultants, agency workers, volunteers, and any other individuals engaged to perform services for or on behalf of the University or its affiliated entities.
- Third parties: Suppliers, research collaborators, agents, and delivery partners, particularly where activities involve elevated fraud or economic crime risk.

The scope of this Policy extends to both UK-based and international operations.

DEFINITIONS OF KEY TERMS

- **Economic Crime:** For the purposes of this Policy includes cheating the public revenue, false accounting, false disclosures, obtaining services dishonestly, false directors' statements, abuse by position, false representation, fraudulent trading, money laundering and illicit finance, embezzlement.
- **Fraud:** Dishonestly making a false representation, failing to disclose information or abusing a position to make a gain or cause a loss.
- **Failure to Prevent Fraud Offence:** A corporate offence where a large organisation fails to prevent fraud by an associated person intended to benefit the organisation (or a related person). A defence exists if the organisation had "reasonable procedures" to prevent fraud.
- **Large Organisation Test:** An organisation is "large" if it meets at least two of the following: (i) >250 employees; (ii) >£36m turnover; (iii) >£18m total assets. (Apply at consolidated group level where relevant.)
- **Associated Person:** Any person who performs services for or on behalf of the University (e.g., staff, agents, subsidiaries, JV partners, contractors, intermediaries).
- **Senior Manager:** An individual who plays a significant role in making decisions about how the whole or a substantial part of the organisation's activities are managed or organised.
- **Reasonable (or Adequate) Procedures:** Risk-based, proportionate procedures informed by a documented fraud risk assessment.
- **MLRO:** Money Laundering Reporting Officer; where appointed, the officer responsible for handling Suspicious Activity Reports (SARs).

Note: Universities are typically **not** in the regulated sector for AML purposes unless engaging in specific regulated activities; however, money-laundering and fraud offences still apply.

ROLES & RESPONSIBILITIES

- **Council:** The Council sets the tone from the top. It commits to the highest standards of ethical conduct and ensures that all University activities reflect the University's values, governance expectations, and defined risk appetite. It approves the Policy and holds the Executive to account for implementation and effectiveness; it receives periodic assurance reports.
- **Audit & Assurance Committee:** Oversees risk management, internal controls, and assurance on economic-crime risks; reviews investigations and lessons learned.
- **Vice-Chancellor / President:** Ensures the implementation of the mandated systems and controls and promotes a culture of integrity.
- **Chief Operating Officer:** Establishes standards for operating human resource controls, data and system controls, and facilities controls, and ensures these are embedded in the organisation.
- **Chief Financial Officer:** Establishes and embeds standards for operating financial controls and procurement controls. Acts as MLRO, receives and evaluates SARs. Liaises with the NCA; maintains SAR records and staff guidance.
- **PVC Research:** Establishes and embeds standards for the operation of research and innovation controls.
- **Chief Student Officer:** Establishes and embeds standards for the operation of student related controls.
- **Vice President Global:** Establishes standards for the operation of Advancement controls and international agent controls, and international collaborations (including transnational education) and ensures these are embedded within the organisation.
- **University Secretary:** Establishes standards for the operation of governance controls, reporting and disclosure controls, and monitoring and assurance controls. Maintains the Policy, framework, and resourcing; ensures

cross-University implementation, reporting, and continuous improvement.

- **All Staff and Associated Persons:** Must comply with this Policy; complete training; conduct due diligence; and report concerns immediately.

MANDATED SYSTEMS AND CONTROLS (RULES)

The following controls are **mandatory**. Faculties, divisions, directorates, subsidiaries, and overseas operations must implement them proportionately to their risk profiles.

Financial Controls

Segregation of Financial Duties

Critical financial processes—such as authorisation, custody of assets, and record-keeping—are separated across different individuals to reduce opportunities for manipulation.

Line Management Review (“Four-Eyes” Check)

All key transactions require a secondary review and approval by a qualified manager.

Suspicious Transaction Detection

Automated and manual reviews detect irregular patterns, potential fraud indicators, or deviations from expected behaviour.

Journal Entry Controls

All manual journal entries require justification, supporting documentation, and an independent review.

Reconciliations

Regular reconciliations of bank accounts, balance-sheet items, and subsidiary ledgers are performed and independently reviewed.

Bank Detail Change Validation

Changes to bank details require formal verification, dual approval, and documented validation checks.

Project Expense Controls

Project expenditures must follow authorised budgets with oversight from project managers and finance.

Ring-Fencing of Funds

Specific funds are segregated and monitored to ensure compliance with donor or contractual restrictions.

Management of Doubtful Contributions

Processes exist to review overdue debts, assess recoverability, and record impairments transparently.

Treasury Record Management

Comprehensive records of cash, investments, borrowing, and treasury activity are maintained securely and consistently.

Financial Counterparty Due Diligence

Formal checks validate the identity, financial standing, and integrity of counterparties before transactions are initiated. Structured due-diligence processes assess third-party integrity, ownership, compliance history, and financial stability.

Tax Risk Identification

Regular reviews identify emerging tax exposures and ensure timely mitigation.

Tax Returns and Disclosures

All tax submissions undergo review and sign-off to ensure completeness and adherence to legislation.

Professional Tax Advice and Auditing

Specialist advisers provide independent tax guidance and conduct audits where required.

HMRC Approval & Dispute Management

Formal procedures manage communications, approvals, and disputes with HMRC, ensuring timely and accurate responses.

Allocation of Expenses (VAT)

Expenses are reviewed and classified correctly for VAT purposes, with oversight by Finance.

Procurement Controls

Procurement Thresholds and Competitive Tendering

Apply defined procurement thresholds to determine when competitive tendering is required and prioritise the use of approved procurement frameworks to ensure fairness and value for money.

Procurement Conflicts of Interest Declarations

To ensure that all individuals involved in procurement activities disclose any actual or potential conflicts of interest so that purchasing decisions remain fair, transparent, and free from undue influence.

Supplier Due Diligence

Conduct proportionate, risk-based due diligence on all suppliers prior to engagement to identify and mitigate potential fraud or compliance risks.

Supplier Identity Verification

Verify the identity and legitimacy of suppliers, including corporate status, ownership, and registration details, before onboarding.

Directed Preferred Suppliers

Use an approved list of preferred suppliers to ensure procurement is conducted with vetted and reliable vendors.

Procurement Delegated Authorities

Apply clear delegated authority limits covering new supplier onboarding, transaction limits, and the approval of purchase orders to ensure appropriate oversight.

Procurement Contractual Agreements

Include robust contractual clauses addressing fraud, bribery, compliance obligations, audit rights, and clear termination rights for misconduct or breach.

Supplier Performance Monitoring

Perform periodic reviews of supplier performance and risk indicators to confirm ongoing suitability and compliance.

Supplier Account Verification

Verify supplier bank account details independently before setup and prohibit payments to unverified or altered accounts.

Procurement Reconciliations

Regularly reconcile invoices, purchase orders, and payment records to identify discrepancies, errors, or signs of fraud. Use a three-way matching process (purchase order, goods receipt, and invoice) to validate the accuracy and legitimacy of payments.

Third-Party Crime Insurance

A crime insurance policy provides coverage for losses arising from external fraud, theft, or dishonesty.

Human Resource Controls

Pre Employment Due Diligence

Conduct comprehensive pre-employment checks—such as identity verification, right-to-work confirmation, qualification checks, and reference validation—to ensure the legitimacy and suitability of candidates.

Temporary, Casual, and Agency Staff Due Diligence

Apply consistent onboarding, screening, and tracking processes for all non-permanent staff to ensure compliance with employment law, right-to-work requirements, and pay parity expectations.

Hiring Conflict of Interest Declarations

Require staff involved in hiring, promotion, or reward decisions to declare actual or potential conflicts of interest and ensure appropriate mitigation is applied to protect decision integrity.

Hiring Delegated Authorities

Define clear delegated authority levels for approvals related to hiring, contract changes, salary adjustments, and role creation to ensure decisions are authorised and appropriately governed.

Job Evaluation and Pay Frameworks

GOVERNANCE DOCUMENTATION

Policy for Security Against Economic Crime
2026/2027

Use fair, consistent, and transparent job evaluation processes and pay structures to ensure salaries and grading decisions are equitable and defensible.

Staff Performance Management

Maintain structured performance management processes—including objective setting, regular reviews, and documentation—to support accountability, employee development, and early identification of performance concerns.

Compliance Training

Ensure employees complete mandatory induction and refresher training (e.g., safeguarding, data protection, equality and diversity) and maintain accurate records to demonstrate institutional compliance. Targeted training for higher risk roles.

Workforce Recordkeeping

Maintain complete, accurate, and up-to-date HR records—covering employment contracts, training, performance, and compensation—to support governance, reporting, and audit readiness.

Payroll Reconciliation

Embed controls to ensure payroll accuracy, segregation of duties, and timely reconciliation between HR data and payroll systems, preventing fraud, error, or unauthorised payments.

Disciplinary Framework

Ensure that all allegations of misconduct are managed through a fair, transparent, and consistent disciplinary process that upholds organisational policies, protects the rights of individuals, maintains compliance with employment legislation, and supports a safe, respectful, and accountable working environment.

Exit Processes and Offboarding

Implement structured offboarding processes—including return of assets, removal of system access, and exit interviews—to reduce security risks and support workforce insights.

Information Systems Controls

User Account Management

Formal creation, maintenance, and removal of user accounts based on role and business need.

System Access Controls

Access privileges reflect the principle of least privilege and are aligned to job responsibilities. Finance, HR, payroll, and research systems have enhanced access controls and approval workflows.

Multi-Factor Authentication

Required for all sensitive and high-risk systems, including email and remote access.

User Profiling and Intended-Use Verification

Regular validation that users only access systems consistent with authorised and expected work activities.

IT Asset Lifecycle Management

Controlled provisioning, tracking, and secure return of devices and system resources.

Information Classification

Data labelled and managed according to sensitivity, with rules for storage, transmission, and sharing.

Secure Data Sharing

Access to and distribution of data restricted to the minimum necessary for legitimate business functions.

System and Transaction Monitoring

Comprehensive logs for key transactions, privileged user activity, and high-risk operations. Logs are tamper-evident, retained for an appropriate period, and available to support investigations. Monitoring for unusual patterns, suspicious behaviour, or potential misuse of IT systems.

Email and Payment-Redirection Protection

Controls to prevent phishing, spoofing, and business email compromise attacks such as payment diversion.

Research and Innovation Controls

Due Diligence on Research Partners, Collaborators, and Funders

GOVERNANCE DOCUMENTATION

Policy for Security Against Economic Crime
2026/2027

Perform due diligence to assess the integrity, financial stability, reputation, and regulatory compliance of proposed research partners and funders.

Research Conflicts of Interest Declarations

Require researchers, reviewers, and decision-makers to declare actual or potential conflicts of interest to maintain transparency and integrity in research collaborations.

Delegated Authorities for Research Funders

Apply structured controls over grant acceptance, including review of terms, compliance obligations.

Research Application Approval

Ensure all research funding applications undergo formal review and approval to validate eligibility, strategic alignment, and compliance with internal and external requirements. Subject grant proposals to peer review to ensure scientific merit, methodological rigour, and adherence to ethical and quality standards.

Research Funding Agreements

Ensure that all research funding agreements entered with universities are developed, reviewed, approved, and monitored in a consistent, compliant, and transparent manner.

Research Collaborative Agreements

Ensure all research collaboration agreements (RCAs) are initiated, negotiated, executed, and monitored in a consistent, compliant, and transparent manner that protects the organisation's legal, financial, IP, data privacy, security, and reputational interests.

Monitoring of Research Partners, Collaborators, and Subcontractors

Monitor subcontractors and external delivery partners to ensure research is conducted to agreed standards, timelines, and compliance expectations.

Research & Innovation Project Audits

Implement periodic audits of research projects to assess compliance, data integrity, financial management, and adherence to grant terms.

Research Transaction Reconciliations

Conduct regular reconciliations of research budgets to monitor spending, identify variances, and ensure funds are used in accordance with grant conditions.

Delegated Authorities for Research Projects

Apply clear delegated authority levels to the approval of research capital spending to maintain financial control and accountability.

Advancement Controls

Due Diligence on Philanthropic Donations

Conduct proportionate due diligence on all funds raised to verify legitimacy, identify potential ethical or reputational risks, and confirm alignment with university values. Perform proportionate, risk-based due diligence on donors—including deep background checks where necessary—to assess financial legitimacy, reputational considerations, and potential conflicts with institutional values.

Philanthropic Donations Conflict of Interest Declarations

To ensure that donations offered to the organisation are transparently declared and assessed for potential conflicts of interest, safeguarding the integrity, independence, and impartiality of organisational decision-making.

Donation Agreements

Include explicit statements in gift agreements ensuring that donations cannot influence teaching, research, governance, or academic freedom. Include contractual clauses that permit the university to refuse, suspend, or return funds if risks emerge later—such as legal issues, reputational threats, or breaches of agreement.

Delegated Authority for Philanthropic Donation Acceptance, Conditional Acceptance or Refusal

Apply clear delegated authority levels governing who may approve, decline, or escalate gift

acceptance decisions to ensure proper oversight and risk management.

Gift Aid Verification and Income Allocation

Obtain and hold records of up-to-date Gift Aid declarations, to enable verification of eligibility for Gift Aid claims and processing of Gift Aid claims in compliance with HMRC regulations, to maximise allowable benefits while maintaining regulatory adherence. Gift Aid claims are supported by valid donor declarations and subject to verification checks.

Philanthropic Donation Record Keeping

Maintain accurate, timely, and transparent records of all gifts, including donor details, restrictions, and reporting obligations, ensuring visibility for internal and external audit requirements. Document and agree the specific purposes, conditions, and allowable uses for each gift to ensure funds are applied ethically and in accordance with donor intent and university policies.

Agent Controls

Due Diligence of Recruitment Agents

Conduct due diligence, performance monitoring, and compliance oversight of international recruitment agents to prevent fraud, misrepresentation, or undue influence.

Recruitment Agent Conflict of Interest Declarations

To ensure that individuals involved in appointing, managing, or overseeing international agents disclose any actual or potential conflicts of interest, so that recruitment and partnership decisions remain transparent, impartial, and free from undue influence.

Delegated Authority for Appointment of Agents

Apply clear delegated authority levels governing who may approve, decline, or escalate appointment of agent decisions to ensure proper oversight and risk management.

Agent Legal Agreements

The University must ensure that all international agents operate under legally binding agreements that clearly set out anti-bribery, anti-fraud,

anti-money laundering, and ethical conduct obligations. These agreements must explicitly prohibit corrupt practices, improper financial incentives, undisclosed commissions, and any activity that could expose the University to economic crime risks.

Monitoring of Agents

Track, review, and validate the commission structures, payments, performance activities, and contractual compliance of all agents and international recruitment partners. Monitoring should detect anomalies, ensure adherence to approved fee arrangements, and provide assurance that partner behaviour aligns with ethical, regulatory, and financial-crime requirements.

Student Admissions and Admin Controls

Admissions Criteria and Selection

Maintain transparent, documented admissions criteria and selection processes to ensure fairness, prevent manipulation, and reduce the risk of fraudulent or improperly influenced admissions decisions.

Right-to-Study Verification

Conduct legally required right-to-study checks for all applicants and returning students to confirm eligibility and prevent fraudulent enrolments.

Random Credibility Assessments

Perform randomised credibility checks on applicants to strengthen fraud prevention and detect fabricated information or false representations.

Identity Verification at Admissions

Verify student identity through reliable documentation and secure processes at both admission and enrolment stages to prevent impersonation or fraudulent registration.

Hardship Funds, Bursaries, and Scholarships Due Diligence

Use proportionate due diligence, eligibility checks, and approval processes to ensure awards are

GOVERNANCE DOCUMENTATION

Policy for Security Against Economic Crime
2026/2027

granted legitimately and are not exploited for fraudulent purposes.

Student Expulsions for Misconduct or Fraud

Ensure expulsions relating to fraud, misconduct, or compliance breaches follow a transparent and legally robust disciplinary process.

Student Complaints Handling

Maintain a transparent, documented complaints process with appropriate oversight to identify patterns of behaviour or fraud-related concerns.

Student Finance Controls

Student Invoicing

Ensure invoices issued to students are accurate, timely, and subject to segregation of duties and reconciliation processes.

Student Fee Adjustment Control

Apply controlled, transparent fee recalculation procedures—such as those related to changes in enrolment status—to prevent manipulation or error.

Refund Management Control

Use documented, transparent refund procedures that require proper authorisation and verification to reduce the risk of fraud or error.

Tuition Fee Payment Controls

Apply financial controls over tuition payments—including verification, reconciliation, and exception monitoring—to identify unusual or suspicious transactions.

Accommodation Fee Payment Controls

Maintain standardised controls for collection, reconciliation, and monitoring of accommodation payments to ensure accuracy and detect potential payment-related fraud.

Other Student Fees and Charges Control

Ensure all student-related fees (e.g., ancillary charges) are documented, approved, communicated clearly, and subject to appropriate financial controls.

Student Debt and Defaults Control

Implement structured processes for monitoring overdue balances, managing student defaults, and applying consistent escalation and recovery procedures. Apply consistent late-payment policies and monitoring processes to ensure timely intervention and prevent concealment of fraudulent activity.

Monitoring of Unusual Payment Patterns

Monitor for unusual or high-risk payment behaviours (e.g., large cash payments, payments from high-risk jurisdictions) and escalate where necessary.

Disclosure and Reporting Controls

Whistleblowing

Formal whistleblowing procedure that enables individuals to confidentially raise concerns about suspected wrongdoing.

Suspicious Activity Reporting

Structured procedures for staff to recognise, document, and escalate unusual or suspicious activity. Ensure clear criteria, reporting routes, and mandatory escalation timelines. Assessing and investigating suspicious activity reports.

Conflicts of Interest Declaration

Disclose any actual, potential, or perceived conflicts of interest, safeguarding the integrity, fairness, and transparency of decisions. Assess and determine mitigations.

Annual Statement on Internal Control Arrangements

To provide independent assurance that fraud controls are operating effectively and that significant risks or deficiencies have been identified and addressed. Produce a formal annual statement summarising the organisation's fraud-control environment, control effectiveness, incidents, and improvement actions.

Governance Controls

Director Identity Verification

GOVERNANCE DOCUMENTATION

Policy for Security Against Economic Crime
2026/2027

Ensure the legal identity of every director (including interim and permanent executive and non-executive directors) is verified using reliable, independent sources before appointment and upon material change, to prevent impersonation, fraud, and regulatory non-compliance.

Director Fitness and Propriety Checks

Ensure directors (executive and non-executive) are (and remain) fit and proper—demonstrating integrity, competence, financial soundness, and absence of disqualifying factors—prior to appointment and on an ongoing basis.

Non-Executive and Executive Director Conflicts of Interest Declaration

Ensure actual, potential, and perceived conflicts of interest involving directors are identified, declared, recorded, assessed, and appropriately managed to protect the organisation's independence, decision quality, and stakeholder trust.

Finance Committee

Implement formal oversight by designated governance bodies for all financial transactions ensuring decisions are transparent, appropriately authorised, and supported by due diligence. Subject all capital spending, intragroup capital transactions, investment transactions and loan agreements to appropriate review, approval, and oversight mechanisms, ensuring risk assessment, proper documentation, and compliance with organisational policies.

Remuneration Committee

Maintain structured oversight of all pay-related decisions, including salary changes, bonuses, and incentives, through appropriate approval pathways and documentation standards.

Nominations and Governance Committee

Maintain structured oversight of all director nominations, through appropriate pathways and documentation standards. This should include oversight of fitness and propriety, declarations of conflicts of interest, oversight of identity verifications.

Group Oversight

Subsidiary formation requires due diligence, risk assessment, and approval by designated governance bodies. Oversight of divestments and mergers.

Delegation of Authorities

A structured delegation of authority matrix sets approval thresholds for remuneration decisions, nomination decisions, expenditure, contracts, financial commitments, and divestments and mergers.

Monitoring, Metrics, and Assurance

Key Risk Indicator Monitoring

To detect early signs of fraud or control breakdowns through regular monitoring of high-risk metrics and timely escalation of anomalies. Monitor key risk indicators such as payment-variation spikes, bank-detail-change rates, duplicate payments, high-risk vendor counts, phishing-click rates, and exceptions in grant claims.

Risk Assessment

To proactively identify, evaluate, and prioritise fraud risks so that controls can be designed, enhanced, or targeted to mitigate emerging threats. Conduct assessments to identify fraud vulnerabilities, evaluate the effectiveness of existing controls, and inform mitigation plans and resource allocation.

Internal Audit

To ensure fraud-related processes and controls are evaluated impartially, identifying weaknesses or gaps. Commission periodic reviews by internal audit or external specialists to assess the robustness of fraud risk management, control design, and operational effectiveness.

Related Documents

The following are not publicly available and are intended for staff and associated parties only.

Please consult the relevant manuals for guidance on the standardised operation of mandated controls, ensuring alignment with Council expectations.

- Financial Control Standards Handbook
- Procurement Control Standards Handbook
- Human Resource Control Standards Handbook
- Information Technology Control Standards Handbook
- Research and Innovation Control Standards Handbook
- International Agency Control Standards Handbook
- International Education Control Standards Handbook
- Advancement Control Standards Handbook
- Student Admissions Control Standards Handbook
- Student Registration Controls Standards Handbook
- Academic Performance, Quality and Governance Control Standards Handbook
- Governance and Assurance Control Standards Handbook

Document Control

Policy Owner: Chief Operating Officer

Policy Administrator: University Secretary

Approved by: Council

Version history:

Version	Date	Description of Change
1.0	May 2026	Original

Next Review Date: May 2029

Additional reviews will be undertaken if there is a material change to the operating model or a material external event.