2011 Review of Assurance and Risk Management Services

The attached review of the Assurance and Risk Management Services section was undertaken from 1 – 3 November 2011.

As indicated, the review recommended that, in order for the University to fully achieve its institutional objectives, there was a necessity to make changes to UQ's organisational arrangements for internal audit, risk management and investigations.

A key principle underlying the review recommendations is the 'three lines of defence' model, recognised as being industry best practice:

- First Line – operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risk
- Second Line – the Enterprise Risk function facilitates and monitors the implementation of effective risk management practices by operational management, and assists the risk owners in reporting risk related information up and down the organisation
- Third Line – Internal Auditing will, through a risk based approach, provide assurance to the organisation's governing body and senior management

The review report initially recommended that the three lines of defence model would be achieved through the reorganisation of the existing Assurance and Risk Management Services into two units (Internal Audit and Investigations, and Enterprise Risk Management).

However, after subsequent consideration of these recommendations, the review committee agreed that the decision to establish three areas each led by associate director positions would best support the 'three lines of defence' model. Under the revised structure, all three associate directors have direct and open access to the Chancellor, Vice-Chancellor and the Chair of the Senate Risk Committee.

The revised organisational structure was also noted by the Senate Risk Committee and endorsed by Senate. The CMC received a copy of the review report and were briefed on the implementation of the recommendations, including the proposed restructure.

Professor Deborah Terry
Vice-Chancellor

REPORT TO THE VICE-CHANCELLOR
BY THE REVIEW COMMITTEE

Assurance and Risk Management Services

1 to 3 November 2011

CONTENTS

Page

TERMS OF REFERENCE

1. Assess whether the identified functions, scope and goals of the unit are consistent with the University's strategic objectives and meet industry best practice.

2. Identify the University's and relevant external agency's service expectations of ARMS; assess the validity of the expectations; and assess ARMS' ability to meet them.

3. Review ARMS' efficiency and effectiveness in meeting its assurance function, enterprise risk management co-ordination, its investigation process, planning, working papers, reporting and coverage.

4. Review the scope of current and planned work and the mechanisms by which priorities are developed and approved.

5. Seek and evaluate views on the scope, focus and service provision of ARMS from the University and the Risk Committee and identify strengths and opportunities for improvement.

6. Identify the optimum organisational structure of the unit in the context of its functions, anticipated developments, and in the context of the University's governance structure and broader industry practice for risk and assurance management.

7. Evaluate whether the profile and skill base of the current staffing structure can appropriately meet its functions and goals, now and into the future.

8. Assess the systems and level of resources needed for ARMS to achieve its identified functions and goals.

9. Identify key performance indicators for future evaluation.

10. Assess the level of independence from Management in which ARMS operates.

Approved by the Vice-Chancellor's Executive on 1 August 2011

MEMBERSHIP OF THE REVIEW COMMITTEE

External Members	Dr Len Gainsford (Chair) Director, Audit and Assurance Department of Transport State Government of Victoria
	Mr Edward Ho Director, Internal Audit The University of New South Wales
Internal Members	Ms Shard Lorenzo Director, Human Resources Division The University of Queensland
	Professor Alan Rix Pro-Vice-Chancellor The University of Queensland
Secretary	Ms Karen Wheeler Director, Academic Administration The University of Queensland

SUMMARY OF RECOMMENDATIONS

1. ROLES AND RESPONSIBILITIES

Recommendation 1

(a) That the draft ARMS Charter recently endorsed by the Senate Risk Committee be independently reviewed and re-named as the Audit and Investigations Charter. The review should consider alignment with the 2011 Senate Risk Committee Charter and model Charters, such as that provided by the Institute of Internal Auditors (IIA);

(b) Consistent with the IIA International Professional Practices Framework (IPPF) Standard 1300, a Quality Assurance and Improvement Program for UQ's audit and investigations function be designed and implemented by 31 March 2012; and

(c) Following these two actions, an External Quality Review of the operation of the audit and investigations function under the terms of the IIA's IPPF is conducted by the IIA by 30 June 2012. The Review Committee agreed that aspects under its Terms of Reference 3, 7, 8 and 9 (refer page 3) could also be dealt with in more detail as part of the External Quality Review.

2. UNIVERSITY GOVERNANCE AND RISK

Recommendation 2

In the light of changes to University governance and risk objectives, the Review Committee has considered the key functions of audit, risk, compliance and investigations in achieving effectiveness.

The Committee recommends:

(a) that compliance, Enterprise Risk Management, audit and investigations functions be reorganised as follows:

- *a legal compliance framework be developed consistent with the Australian and New Zealand standard on Compliance Programs AS/NZS 3806;*
- *the UQ legal compliance framework is managed by the University Legal Office;*
- *Enterprise Risk Management report direct to the Executive Director Operations (EDO), and separately to the Chair of the Senate Risk Committee;*
- *the Director internal audit and investigations reports functionally to the Vice-Chancellor and separately to the Chair of the Senate Risk Committee, and to the EDO on administrative matters;*
- *the EDO is appointed as an additional UQ/CMC Liaison Officer; and*
- *an Investigations Reference Group be established under a Terms of Reference to oversee the UQ investigations program and its priorities.*

This means, in a structural sense:

- *that a legal compliance officer be appointed to the Legal Office with the objective of providing advice and assistance to managers across the University in meeting their compliance obligations;*
- *that an Enterprise Risk Management Unit be established and adequately resourced. The key responsibility is to facilitate and monitor effective risk management by University management and provide regular reports to the USMC Risk Committee and Senate Risk Committee; and*

- *that an Internal Audit and Investigations Unit (AIU), including investigations, be established and adequately resourced. The key responsibility of the AIU is to provide independent and objective reviews and reporting on internal controls and recommending improvements.*

(b) that selected internal audits be contracted out, as appropriate, on the basis of an approved annual audit plan. Investigations be contracted out on the basis of workload, sensitivity and specialist expertise;

(c) that a competency framework be developed and implemented for the future leadership and staffing of the audit, investigations, risk and compliance functions as set out above; and

(d) that the Investigations Reference Group include a member of the Vice-Chancellor's Executive, the Executive Director (Operations) and University Secretary, the University Lawyer, Director Human Resources and the relevant position from the audit and investigations area.

3. ENTERPRISE RISK MANAGEMENT (ERM)

Recommendation 3

That, in acknowledging the importance of risk and risk management to the governance of the institution:

- *the University endorses the importance of the enterprise risk register and risk management processes, but recognises that the important business-as-usual aspects of operational risk management (including the systems used) need to be more closely aligned with enterprise risk;*
- *a closer relationship be forged in the Faculties, Institutes and Divisions between risk management activities and the University's strategic and operational planning processes; and*
- *the University goes to the next stage in development of the risk management process by increasing the focus on risk appetite, risk tolerance, emerging risks and external relationship.*

4. ALIGNMENT OF RISK MANAGEMENT AND INTERNAL AUDIT ACTIVITIES WITH STRATEGIC AND OPERATING PLANS

Recommendation 4

It is proposed:

(a) that the annual risk assessment exercise, the updating of the risk registers, and the formulation of the internal audit plan be synchronised with UQ's strategic and operational planning cycle;

(b) that in addition to risks relating to business-as-usual activities, the risk identification process be driven by the objectives in UQ's strategic and operating plans, involving the identification of those risks that may emerge in the course of UQ achieving its plan objectives and the linkage of these objectives and risks explicitly articulated in the risk registers;

(c) that in addition to the risk registers which inform the internal audit plan, Internal Audit consult with the members of the USMC, the Risk Committee, the Chair of the Finance Committee, and the Queensland Audit Office in regards to UQ's activities and issues where internal audit reviews are required to provide independent assurance on the effectiveness of internal controls;

(d) that the process of engagement in c) above be used as a forum to assess the adequacy of internal audit resources and their prioritisation;

(e) that the internal audit plan covers a three year period which is to be updated annually;

(f) that the internal audit plan includes a list of internal audit reviews to be performed over the three year period. For each review listed, there will be a summary of scope, objectives and the rationale for that review to be performed; and

(g) that the three year internal audit plan (including annual updating) be endorsed by the Vice-Chancellor and then approved by the Risk Committee consistent with the Risk Committee Charter.

5. CONTROLLED ENTITIES: GOVERNANCE, RISK MANAGEMENT AND INTERNAL AUDIT LINKAGES

Recommendation 5

That the University's Enterprise Risk Management function extends its scope to consideration of the impact of controlled entities on the University's risk profile, subject to appropriate understandings between the University and UQ Holdings on such assessments.

6. OCCUPATIONAL HEALTH AND SAFETY

Recommendation 6

In the light of the introduction of unified national OH&S legislation, that the Senate Risk Committee consider how it might best receive regular advice on occupational health and safety, given that it has been identified as the USMC Risk Sub-Committee's top current strategic risk.

7. ASSURANCE FRAMEWORK

Recommendation 7

(a) that the UQ Director, Audit and Investigations, in consultation with the Chair of the Senate Risk Committee, develops an assurance framework including an opinion formulation process, such that appropriate opinions on risk and internal controls by designated assurors are able to be formed and reported to the Risk Committee;

(b) that the UQ Director, Audit and Investigations, in consultation with the Chair of the Senate Risk Committee, design a framework whereby management is primarily responsible for the provision of assurance opinion on risk and internal controls, but where independent assurance for certain risk activities is provided by internal audit. The determination of areas where independent assurance is required will take place at the time when the three year internal audit plan is formulated or updated (refer Section 4);

(c) that the 26 August 2010 UQ Risk Committee of Senate Charter and the 2005 ARMS Charter be amended to reflect the formulation, delivery and receipt of assurance opinions recommended above; and

(d) that these actions be reflected in the Quality Assurance and Improvement Program for the UQ's audit and investigations function to be designed and implemented by 31 March 2012.

8. RELEVANCE TO STAKEHOLDERS' ACTIVITIES

Recommendation 8

(a) that during the consultation process when the annual internal audit plan is formulated or updated (refer Section 4), Internal Audit seeks advice from the stakeholders of any specific requests where Internal Audit's input is required for new initiatives or improvement of current activities;
(b) that consideration be given to package these requests into reviews where the scope and objectives focus on control designs which are relevant to the immediate needs of the operations or provide proactive support to new initiatives; and
(c) that the process for the formulation or updating of the annual internal audit plan (refer Section 4) involves engagement with members of senior management and relevant Senate Committees.

9. PROPOSED INTEGRITY OFFICE

Recommendation 9

That the ARMS proposal that an Integrity Office be established within ARMS not be supported, but that the current University arrangements for overseeing integrity be maintained. The annual approved internal audit and investigation plan needs to include regular reviews of probity. In addition, probity matters should be subject to oversight by the proposed Investigations Reference Group.

REPORT OF THE REVIEW COMMITTEE

PROCEDURE

The Review Committee met and conducted interviews during the period 1 to 3 November 2011. The Committee undertook its work under the approved Terms of Reference, while taking into account written submissions and other background materials supplied by The University of Queensland (UQ).

A brief site visit was conducted of the ARMS Unit, which included an informal lunch with staff. Other brief site visits were conducted of the Queensland Brain Institute, as well as a laboratory in the School of Chemistry and Molecular Biosciences.

The Review Committee held meetings with senators and senior officers of the University, management and members of staff of the Unit.

In finalising its report, the Review Committee presented the major themes and a summary of draft recommendations to the Executive Director (Operations) and University Secretary.

The Review Committee also presented the major themes and a summary of the preliminary findings at a meeting to which all staff of the Unit were invited.

EXECUTIVE SUMMARY

The Review Committee acknowledges the contribution that the Unit has made to the University since it was established and is mindful of the current and changing context of assurance and risk management services. It is within this context and framed by the objective of directly supporting the University's goals (as outlined in the UQ Strategic Directions and 2011-15 Plan) that the Committee has considered the activities undertaken by the ARMS Unit.

The Committee believes the Unit has the potential to continue to add value to the operations of the University; however this must be informed by strategic leadership, planning and an appropriate structure. For future and continued relevance, the Unit's role must be organised in such a way as to ensure the capacity for flexibility and adaptability to deal with ongoing changes.

As a key principle, the Committee considered that any model implemented by the University should reflect best practice in corporate governance, whereby the identification and management of risk is linked to the achievement of institutional objectives, and the approach to internal control is risk-based, with risk assessment and internal controls embedded in ongoing operations. The Committee considers this to be an important opportunity for the Unit and the University more broadly to actively contribute in this area.

The development of an improved operational structure is considered important. The operational style adopted by the enterprise risk management and the assurance and investigations functions is increasingly relevant to how University outcomes are achieved. Particular themes involve problem solving, preventative actions, the formation of value-adding partnerships and assistance with compliance activities.

Nine recommendations are provided to the Vice-Chancellor for consideration and focus on alignment of the Unit's priorities to those of the University's Strategic Plan. The Review Committee grouped its recommendations into the following areas:

- Roles and Responsibilities
- University Governance and Risk
- Enterprise Risk Management (ERM)
- Alignment of Risk Management and Internal Audit Activities with Strategic and Operating Plans
- Controlled Entities: Governance, Risk Management and Internal Audit Linkages
- Occupational Health and Safety
- Assurance Framework
- Relevance to Stakeholders' Activities
- Proposed Integrity Office

The Review Committee formed the view that the Unit has made a very important and useful contribution to the University. However, in order for the University to fully achieve its institutional objectives, changes in emphasis, organisational and management structure are required. The Review Committee proposes that this report will provide the context and impetus for these changes to occur.

COMMENDATIONS

During the process of the Review, the Review Committee noted and received considerable positive comment on several aspects related to staff, services and operations of the Unit.

The Review Committee considers that the following specific commendations are well deserved by the ARMS Unit. These are not necessarily in order of importance.

Commendation 1: *The Senate Risk and Finance Committees' strong emphasis on enterprise risk management is widely supported and serves as a strong foundation for changes across the University.*

Commendation 2: *ARMS is widely respected by managers across UQ. The Unit consists of a committed and dedicated team which has been in place over a long period.*

Commendation 3: *ARMS has responded well to recent governance initiatives in enterprise risk management.*

Commendation 4: *Self-assessment of risks and internal audit outputs have served as a good reminder of key operational controls.*

Commendation 5: *In terms of the acceptance and implementation of the ERM, University staff are willing to work together, share information and hold a commitment to work towards a common goal.*

Commendation 6: *The expertise relating to IT audits is well regarded.*

Commendation 7: *The introduction of a risk management framework and development of commitment towards its progress has been effective. Still further development is required but progress has been pleasing and encouraging. There is a willingness to consider how other features such as risk appetite and risk tolerance might be addressed.*

ISSUES AND RECOMMENDATIONS

1. Roles and Responsibilities

It is clear that arrangements constituting UQ's Senate Risk Committee and UQ's audit and investigations function need to be comprehensive and kept up-to-date. An updated Charter for the Risk Committee of the UQ Senate was completed on 27 July 2010 and approved by the University Senate on 26 August 2010. The Review Committee was told that an updated version of the 2005 ARMS Charter had been endorsed by the University's Senate Risk Committee and that it was awaiting approval by the Senate. The Review Committee confirmed with the Senate Risk Committee Chair that ARMS activities continue to be performed in line with University Policy 1.40.4 *Assurance and Risk Management Services Charter* (currently listed in the Handbook of University Policies and Procedures).

Findings

The Review Committee finds that the 2005 ARMS Charter is out-of-date in referring to the *Financial Administration and Audit Act* (Qld) 1977 and the Financial Management Standard Qld 1997 (at section 1.2); the relationship with the previously named UQ Senate Audit Committee (at section 5.3); the relationship with UQ's Risk Committee (at section 5.4); applicable Standards (at section 6.2); and quality assurance and improvement processes (at section 6.3). The draft ARMS Charter shown at Appendix 2 to the ARMS written submission provides some updating, but it is noticeable that the section on review and assurance process has been deleted.

The Committee finds that an update of the 2005 ARMS Charter should now incorporate provisions under the January 2009 Institute of Internal Auditors' (IIA) International Professional Practices Framework (IPPF), taking into account amendments up to and including those made in January 2011. In particular, it should refer to IPPF Standard 1000–*Purpose, Authority and Responsibility* and also to IPPF Practice Advisory 1000–1 *Internal Audit Charter*.

In the ARMS 2011 Strategic Plan published on the UQ website, it is said that "significantly, 28% of our resources are committed to the Systems Assurance". Although there is mention of Standards and practice statements issued by the Information Systems Audit and Control Association (ISACA) at sub-section 6.2.1 of the 2005 ARMS Charter, the Committee notes there is no mention of quality and improvement procedures to meet ISACA requirements. This should now be addressed.

The Queensland Auditor-General in his 4 October 2011 written submission asked the Committee to consider Auditing Standard ASA 610 *Considering the Work of Internal Audit* in its deliberations. While the published material clearly points to implications of this Standard for UQ, the Committee

notes it is unable to detect any specific reference to it in the 2005 ARMS Charter under section 5.5-Relationship with External Audit. The 22 February 2011 UQ Senate Finance Committee Terms of Reference is also silent on the extent of the external auditor's reliance on the work of UQ ARMS and particularly, its internal audit function. This should now be addressed.

At page 3 of the September 2011 Report on Self-Assessment of ARMS at UQ, the Director ARMS opined that ARMS generally complies with three sub-items under IPPF 1300 Quality Assurance and Improvement Program (QAIP), partially complies with four sub-items and does not have any "does not comply" sub-items. At page 29 to the ARMS written submission it was said that "whilst we have not developed a structured quality assurance program, ARMS is committed to continuous improvement both in its audit procedures and management and administration". This view was confirmed in discussion with the Director ARMS.

The Committee notes that a formal QAIP is mandatory for a Chief Audit Executive under IPPF Standard 1300. It finds that such a program for UQ's audit and investigations function needs to be designed and implemented without delay. As per the Standard, the QAIP includes periodic internal and external assessments and ongoing internal monitoring. Each part of the program should be designed to help internal audit add value and improve the organisation's operations and to provide assurance that internal audit is in conformity with the Standards and the Code of Ethics.

Recommendation 1

(d) That the draft ARMS Charter recently endorsed by the Senate Risk Committee be independently reviewed and re-named as the Audit and Investigations Charter. The review should consider alignment with the 2011 Senate Risk Committee Charter and model Charters, such as that provided by the Institute of Internal Auditors (IIA);

(e) Consistent with the IIA International Professional Practices Framework (IPPF) Standard 1300, a Quality Assurance and Improvement Program for UQ's audit and investigations function be designed and implemented by 31 March 2012; and

(f) Following these two actions, an External Quality Review of the operation of the audit and investigations function under the terms of the IIA's IPPF is conducted by the IIA by 30 June 2012. The Review Committee agreed that Terms of Reference 3, 7, 8 and 9 (refer page 3) could also be dealt with in more detail as part of the External Quality Review.

2. University Governance and Risk

In considering Term of Reference 6 about the organisational structure of the Unit in relation to its functions, the Committee was very mindful of that, with the advent of the new Senate in 2010, the Committees of Senate had been restructured and Committee roles and responsibilities refocussed. What had been the Audit and Risk Committee became the Risk Committee, and the external audit

oversight function moved to the Senate Finance Committee. A Risk Committee of the University Senior Management Committee (USMC) was also established.

This structure placed "risk" at the centre of the Senate's concerns in the assurance portfolio, and marked an important change in philosophy on the part of the Senate's approach to these matters. What had been a process in which investigations tended to be the dominant "audit" function was re-cast to focus on risk as the primary concern of the institution, from which assurance, audit and investigations then flowed. Understanding the risks to the institution is now of paramount concern to the governing body. Having that understanding then allows analysis of the mitigating factors, assurance about controls, and internal audit assurance reviews, if and when necessary. Internal audit assurance reviews need to be linked to the risk-based approach which the Senate now adopts.

This approach reflects practice in corporate governance in higher education, whereby the identification and management of risk is linked to the achievement of institutional objectives, and the approach to internal control is risk-based, with risk assessment and internal controls embedded in ongoing operations.

The approach is also reflected in the Charter of the Senate Risk Committee, which states:

> *1.3 The Committee provides advice and assurance to Senate on the effectiveness of the University's Enterprise Risk Management Framework and the management of risk;*
>
> *1.4 The Committee provides advice, where deemed necessary, to Senate on processes which ensure good governance and it assists Senate in fulfilling its oversight responsibilities for risk management, internal controls, internal audit and assurance.*

At the time of the review, ARMS, headed by the Director ARMS, comprised the functions of enterprise risk management, independent assurance and investigations. The Associate Director ERM Services within ARMS, who reports to Director ARMS, is responsible for the implementation of enterprise risk management across UQ as well as reporting to management and the Risk Committee of Senate on UQ's risk management activities. The Review Committee was advised that the Associate Director ERM also took part in assurance/internal audit activities in addition to a risk management role.

Findings

The development of the University's Enterprise Risk Management activities since 2005, led by the ERM Unit of ARMS, has substantially raised the profile of risk within the University, and has seen a major shift in both understanding of, and action in relation to, risk and risk management. This has occurred at Senate, management and operational levels.

The Risk Committee of the Senate and management of UQ routinely seek independent-of-management assurance from ARMS on the effectiveness of UQ's risk management activities and

internal controls. As "internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations..."[1] the allocation of accountability for risk management and internal control across UQ has to be clearly articulated. In short, it is recognised that "...the two most important ways that internal auditing provides value to the organisation are in providing objective assurance that the major business risks are being managed appropriately and providing assurance that the risk management and internal control framework is operating effectively."[2]

According to page 26 of the ARMS submission, the 2011 ARMS annual budget allocation was $979,000. By comparison, NSW Government internal audit "full service" benchmarking suggests an upper funding envelope of 0.5% of appropriation or, expressed another way, annual total revenue. In UQ's case and considering parent company total revenue, this would amount to an upper limit of $7 million per year. While this upper limit is not advocated in the current circumstances, it nonetheless provides some future direction for resourcing and funding improvements to the Unit's efficiency and effectiveness. The Committee notes from page 28 of the ARMS submission that UQ is the only member of the Group of Eight Universities that does not outsource any part of its annual internal audit program.

In addressing current and future challenges, the Review Committee recognises the *Three Lines of Defence* model, which is advocated by the Institute of Internal Auditors and explained as follows:

> As a **first line** of defence, the institution's operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.
>
> As a **second line** of defence, the risk management function facilitates and monitors the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk related information up and down the organisation.
>
> As a **third line** of defence, internal auditing will, through a risk-based approach, provide assurance to the organisation's governing body and senior management, on how effective the organisation assesses and manages its risks, including the manner in which the first and second lines of defence operate. This assurance task covers all elements of an institution's risk management framework: i.e. from risk identification, risk assessment and – response to communication of risk related information.[3]

---

[1] *Definition of Internal Auditing, Institute of Internal Auditors (IIA)*

[2] *IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management", January 2009, p.3*

[3] *IIA Global Council 2011 Background Paper No.3, Principle 2: "Organisations need clear accountability for risk management and internal control", The Institute of Internal Auditors*

The Senate Risk Committee is able to be assured that the identification and management of risk is operating effectively via an adequately resourced audit and investigations function which operates under the third line of defence. The second line of defence supports reporting of the Enterprise Risk Management function to the operational arm of the University, as well as to the Senate Risk Committee. Similarly, UQ compliance arrangements could be seen functionally and primarily as part of line of defence two, but also with functions spanning the other two lines of defence.

Compliance today is a complex and ubiquitous responsibility that affects all parts of the institution. There is a significant risk for UQ from non-compliance with laws, regulations, standards, policies, processes and established procedures. UQ's management and staff compliance responsibilities include legal compliance with multiple Federal and State laws and administrative instruments covering universities and other state authorities, through to occupational health and safety, environmental, professional, financial and many other areas of university activity. Some parts of the University undertake their own compliance activity without reference to ARMS.

Where there is reference to ARMS, the IIA's Practice Advisory 2400-1 counsels the internal audit activity to exercise caution when communicating non-compliance, and encourages a close working relationship with areas such as the entity's Legal Counsel. To the extent that there are many UQ teaching and research processes which are affected by legislation and regulation, the Review Committee found that legal compliance requires specialist oversight and the provision of advice and assistance by the University Legal Office.

Two other matters were considered in this governance context by the Review Committee. One matter relates to the Crime and Misconduct Commission (CMC), with which the University has regular interactions in relation to matters referred to UQ by the CMC, and matters referred to the CMC by UQ. At present, the Director ARMS is the sole CMC liaison officer. The Review Committee finds that, given UQ's access and continuous communication needs, a single point of contact between UQ and the CMC could be inauspicious and that another senior point of contact should be established.

Another matter concerns investigations. In considering the pattern of investigations, the Review Committee noted a recent "spike" in the number of investigations. It also noted that all investigations were carried out internally to UQ by ARMS. It was found by the Committee that there was no contracting out of services where use of specialist investigative or forensic technologies could have been beneficial to UQ. Further, there was no apparent ARMS mechanism for assessing investigations needs and processes, such that particular investigations under way at any time were not known by key members of UQ executive management. In short, there was no internal Reference Group to consider the type and extent of investigation needs or an Investigation Plan with identifiable decision points.

Recommendation 2

In the light of changes to University governance and risk objectives, the Review Committee has considered the key functions of audit, risk, compliance and investigations in achieving effectiveness.

The Committee recommends:

(e) that compliance, Enterprise Risk Management, audit and investigations functions be reorganised as follows:

- *a legal compliance framework be developed consistent with the Australian and New Zealand standard on Compliance Programs AS/NZS 3806;*
- *the UQ legal compliance framework is managed by the University Legal Office;*
- *Enterprise Risk Management report direct to the Executive Director Operations (EDO), and separately to the Chair of the Senate Risk Committee;*
- *the Director internal audit and investigations reports functionally to the Vice-Chancellor and separately to the Chair of the Senate Risk Committee, and to the EDO on administrative matters;*
- *the EDO is appointed as an additional UQ/CMC Liaison Officer; and*
- *an Investigations Reference Group be established under a Terms of Reference to oversee the UQ investigations program and its priorities.*

This means, in a structural sense:

- *that a legal compliance officer be appointed to the Legal Office with the objective of providing advice and assistance to managers across the University in meeting their compliance obligations;*
- *that an Enterprise Risk Management Unit be established and adequately resourced. The key responsibility is to facilitate and monitor effective risk management by University management and provide regular reports to the USMC Risk Committee and Senate Risk Committee; and*
- *that an Internal Audit and Investigations Unit (AIU), including investigations, be established and adequately resourced. The key responsibility of the AIU is to provide independent and objective reviews and reporting on internal controls and recommending improvements.*

(f) that selected internal audits be contracted out, as appropriate, on the basis of an approved annual audit plan. Investigations be contracted out on the basis of workload, sensitivity and specialist expertise;

(g) that a competency framework be developed and implemented for the future leadership and staffing of the audit, investigations, risk and compliance functions as set out above; and

(h) that the Investigations Reference Group include a member of the Vice-Chancellor's Executive, the Executive Director (Operations) and University Secretary, the University Lawyer, Director Human Resources and the relevant position from the audit and investigations area.

3. Enterprise Risk Management (ERM)

The ARMS submission at pages 17 to 21 makes it clear that the University community has successfully become engaged with the risk assessment and risk management process, as it has been progressed by ERM over recent years. The Committee received many comments warmly endorsing the constructive and supportive process that has been put in place by the Associate Director, ERM, and

of its value to the enterprise and its constituent units. While it is recognised that the development of the risk register and risk management plan are critical for management, at the same time there was criticism expressed of the ERM software and database system that Faculties, Institutes and Divisions are required to use to enter and record their risk profiles. There are a number of suggestions that this was, for many, a "tick and flick" exercise that did not do justice to either the importance of the issues, or the seriousness with which operational units engage in the risk assessment and management process.

Findings

The Review Committee identified a strong recognition of the value of the risk committee governance structures that have been put in place, and the importance of the identification of the "top level" University risks. Similarly, the way in which risk has been incorporated as part of strategic and operational planning is recognised as a valuable step forward for the University, although it was recognised that the challenge now is to ensure that not just the University, but its Faculties, Institutes and Divisions, have the appropriate controls in place to manage their risks, and are continuing to adjust their risk assessments, profiles and controls as circumstances change.

As adjustments take place, risk assessment and management could be expected to become entrenched as an ongoing aspect of University management. Beneficially, it could also lead to more informed discussions of the way in which the University understands risk, plans for risk and accepts and tolerates levels of risk. From the Review Committee's discussions, it would appear that thinking about risk appetite, risk tolerance and emerging risks is part of operational planning, but that there is much yet to be done to advance this discussion at operational levels.

Recommendation 3

That, in acknowledging the importance of risk and risk management to the governance of the institution:

- *the University endorses the importance of the enterprise risk register and risk management processes, but recognises that the important business-as-usual aspects of operational risk management (including the systems used) need to be more closely aligned with enterprise risk;*
- *a closer relationship be forged in the Faculties, Institutes and Divisions between risk management activities and the University's strategic and operational planning processes; and*
- *the University goes to the next stage in development of the risk management process by increasing the focus on risk appetite, risk tolerance, emerging risks and external relationship.*

4. Alignment of Risk Management and Internal Audit Activities with Strategic and Operating Plans

As part of managing enterprise risk, a risk assessment exercise is annually conducted by the University Senior Management Committee (USMC) Risk Sub-Committee. Similarly, the risk registers of the Faculties, Institutes and Divisions are also updated annually.

Findings

Whilst the current Enterprise Risk Management process has gained wide acceptance and considered effective in encouraging the formation of a risk management ethos, the Review Committee has received feedback from the stakeholders that the effectiveness of this exercise will be enhanced if its relevance to operational activities becomes more apparent. In addition, it has been suggested that the annual review exercise of the risk registers at the faculty and school levels appears to focus mainly on risks arising from business-as-usual activities. Some of these risks are deemed by a number of stakeholders to be too generic and that this focus may limit the ability to identify emergent risks.

The internal audit reviews conducted by ARMS are now carried out as per the Annual Audit Plan (referred to in Appendix 12 to the ARMS written submission). The Review Committee was advised that the formulation of the Work Plan was largely informed by the risk registers as updated through the risk assessment exercises. There is limited direct consultation with senior management and members of the Senate Risk Committee and the Finance Committee in the planning process, whereby these key stakeholders are able to provide valuable input into the effective deployment of internal audit resources towards the key risks facing the University.

Currently, the internal audit Work Plan (as per ARMS submission Appendix 12) is for a twelve month period. A twelve month Plan may restrict the ability to plan reviews from a strategic perspective as assurance requirements are driven by the risk profile of UQ's core activities which may evolve over time. A longer term view will enable UQ to identify the optimal timing for a review or series of reviews to be performed to address a particular risk issue. It also allows more effective planning of internal audit resources.

Recommendation 4

It is proposed:

(a) that the annual risk assessment exercise, the updating of the risk registers, and the formulation of the internal audit plan be synchronised with UQ's strategic and operational planning cycle;

(b) that in addition to risks relating to business-as-usual activities, the risk identification process be driven by the objectives in UQ's strategic and operating plans, involving the identification of those risks that may emerge in the course of UQ achieving its plan objectives and the linkage of these objectives and risks explicitly articulated in the risk registers;

(c) that in addition to the risk registers which inform the internal audit plan, Internal Audit consult with the members of the USMC, the Risk Committee, the Chair of the Finance Committee, and the Queensland Audit Office in regards to UQ's activities and issues where internal audit reviews are required to provide independent assurance on the effectiveness of internal controls;

(d) that the process of engagement in c) above be used as a forum to assess the adequacy of internal audit resources and their prioritisation;

(e) that the internal audit plan covers a three year period which is to be updated annually;

(f) that the internal audit plan includes a list of internal audit reviews to be performed over the three year period. For each review listed, there will be a summary of scope, objectives and the rationale for that review to be performed; and

(g) that the three year internal audit plan (including annual updating) be endorsed by the Vice-Chancellor and then approved by the Risk Committee consistent with the Risk Committee Charter.

5. Controlled Entities: Governance, Risk Management and Internal Audit Linkages

The Committee was informed that under the current UQ governance structure, each of the controlled entities of UQ has a governing board of directors. All controlled entities are, or are soon to be, part of UQ Holdings Ltd. The scope of the risk management and assurance activities of ARMS does not now extend to these entities as they are not formally part of the University of Queensland but of its holding company.

Findings

The Review Committee finds that it would be a valuable addition to the University's Enterprise Risk Management function if it were to extend its scope to assess how the current governance framework and the activities of UQ Holdings' controlled entities impact upon UQ's risk profile. This would not involve specific risk assessment of individual controlled entities, but of their operational, tactical and strategic relationship to the University and UQ's risk profile.

The Committee finds that as the governance framework for UQ controlled entities evolves, the role of UQ's enterprise risk management and internal audit functions should be continuously assessed for impact.

Recommendation 5

That the University's Enterprise Risk Management function extends its scope to consideration of the impact of controlled entities on the University's risk profile, subject to appropriate understandings between the University and UQ Holdings on such assessments.

6. Occupational Health and Safety

The University has a comprehensive set of OH&S policies, procedures and guidelines that form its OH&S management system. An integral part of this system is health and safety operational auditing. A primary objective of this auditing is continued improvement of OH&S systems and practices to ensure the University continues to provide a safe and healthy environment for staff, students, contractors, visitors and neighbours.

Findings

The OH&S Unit administers a University-wide proactive accident prevention program using specialist advisers with operational support from within Faculties, Institutes and Divisions. The University manages its own workers' compensation risk through the Self Insurance Program under the auspices of the Work Injury Management team.

The OH&S Unit has grown significantly over the past five years in the breadth of work, the level of responsibility and the requirement to drive change and improvement at a senior level. The OH&S function has moved from a reactive model to a more proactive approach and the University's size, research diversity and technologically sophisticated facilities make it a complex OH&S environment.

It is not surprising that OH&S is identified by the USMC Risk Sub-Committee as the University's top current risk category (at March 2011). In line with this, the recent review of Human Resources has recommended that the OH&S Unit become the OH&S Division lead by a Director OH&S, reporting to the EDO.

In considering the above factors and the introduction of the new national OH&S legislation in 2012, the Review Committee finds that the Senate Risk Committee is best to consider how it receives up-to-date, accurate and comprehensive information regarding OH&S.

Recommendation 6

In the light of the introduction of unified national OH&S legislation, that the Senate Risk Committee consider how it might best receive regular advice on occupational health and safety, given that it has been identified as the USMC Risk Sub-Committee's top current strategic risk.

7. Assurance Framework

Section 6.2 of the 25 August 2011 University Policy 1.80.01 *Enterprise Risk Management* states that "the internal audit function has a role at UQ in assessing the effectiveness of controls over high risk activities". The March 2011 USMC Risk Sub-Committee ranks seven key risks in its Consolidated Register, such as OH&S and environment and incident and crisis management. Such key risks are not specifically identified, nor prioritised, in the ARMS 2011 Operational Plan, or in the ARMS 2011 Review Cycle Risk Register.

Findings

IIA Standard 2410 *Criteria for Communicating* says "Final communication of engagement results must, where appropriate, contain the internal auditors' opinion and/or conclusions. When issued, an opinion or conclusion must take account of the expectations of senior management, the board and other stakeholders, and must be supported by sufficient, reliable, relevant and useful information". In

the 2005 ARMS Charter, there is no mention of internal audit opinion and/or conclusions in section 2-Purpose, section 5.5- Relationship with External Audit or section 7-Review and Assurance Process. There is also no specific mention in the 26 August 2010 Senate Risk Committee Terms of Reference of receiving internal audit opinion and/or conclusions in reporting to the Committee.

As a more positive indication of activity, it is said at page 16 of the ARMS written submission:

> "…with encouragement from the Chancellor and Risk Committee, ARMS has revived development of a program of work to enable us to provide assurance with respect to the soundness of the overall internal control framework. We had commenced such an initiative back in 1995 which was not supported by Management. This has involved an assurance mapping exercise and development of programs for the review of critical systems and controls."

The IPPF Practice Guide *Formulating and Expressing Internal Audit Opinions* assists in the formulation and delivery of internal audit opinion. The Practice Guide refers to the use of grades or ratings in expressing an opinion. Increased precision in the information provided in an opinion normally increases the amount of evidence needed to support the opinion. There is a range of "macro" and "micro" opinion available, including "negative" or "limited" assurance, and "positive" or "reasonable" assurance. Occasionally, internal auditing may be asked for an "informal" or verbal opinion on the adequacy of governance, risk management or control policies and processes. This may be freely given. In any case, opinion needs to be registered and kept for possible use as precedent. Non-opinion forms of assurance such as "factual findings" or "agreed-on-procedures" under Australian Auditing Standards should also be considered for UQ, where appropriate. It is advisable for the UQ Director, Audit and Investigations to discuss these options as part of internal audit Engagement Planning, consistent with IPPF Standard 2200, and IPPF Standard 2400 *Communicating Results*.

The ARMS written submission at Appendix 9, Operational Plan, states that its project "structure and effectiveness of UQ's governance and internal control frameworks" is "20% complete as at 30/9/10". The Committee notes that while the mid-year progress is described as "on track", target dates are now shown as 2011. In the ARMS 2011 Review Cycle Risk Register (shown at Appendix 11 to the ARMS written submission), the likelihood and consequence of ARMS being "ineffective in assisting UQ to manage its high risk areas" is shown as "moderate".

Recommendation 7

(a) that the UQ Director, Audit and Investigations, in consultation with the Chair of the Senate Risk Committee, develops an assurance framework including an opinion formulation process, such that

appropriate opinions on risk and internal controls by designated assurors are able to be formed and reported to the Risk Committee;

(b) that the UQ Director, Audit and Investigations, in consultation with the Chair of the Senate Risk Committee, design a framework whereby management is primarily responsible for the provision of assurance opinion on risk and internal controls, but where independent assurance for certain risk activities is provided by internal audit. The determination of areas where independent assurance is required will take place at the time when the three year internal audit plan is formulated or updated (refer Section 4);

(c) that the 26 August 2010 UQ Risk Committee of Senate Charter and the 2005 ARMS Charter be amended to reflect the formulation, delivery and receipt of assurance opinions recommended above; and

(d) that these actions be reflected in the Quality Assurance and Improvement Program for the UQ's audit and investigations function to be designed and implemented by 31 March 2012.

8. Relevance to Stakeholders' Activities

ARMS' key activities consist of investigations, enterprise risk management, provision of advice, coordination and review of control self-assessments, and internal audit assurance reviews. Comments by the Faculty, Institute and Division representatives indicate that an internal audit function could improve its value-added contribution by forming a stronger connection with their units by increasing the audit function's emphasis on the immediate needs of the operations.

Findings

Whilst use of control self-assessments and the annual update of the risk registers may serve as good reminders in some cases, their impact on value creation and control enhancement is considered low. The internal audit function's engagement with stakeholders across UQ can be deepened by extensively involving the managers and staff of the audited unit when compiling the terms of reference of the individual reviews. In this instance, internal audit, without compromising the independence and rigour of the assurance provided, could invite their colleagues to raise specific control issues or weaknesses where internal audit advice is required, such that the internal audit report will be considered of value and relevance to the audited unit.

Recommendation 8

(a) that during the consultation process when the annual internal audit plan is formulated or updated (refer Section 4), Internal Audit seeks advice from the stakeholders of any specific requests where Internal Audit's input is required for new initiatives or improvement of current activities;
(b) that consideration be given to package these requests into reviews where the scope and objectives focus on control designs which are relevant to the immediate needs of the operations or provide proactive support to new initiatives; and
(c) that the process for the formulation or updating of the annual internal audit plan (refer Section 4) involves engagement with members of senior management and relevant Senate Committees.

9. Proposed Integrity Office

One of the suggestions made in the ARMS' written submission to the Review was that an Integrity Office be established within the ARMS Unit.

Findings

During the course of its deliberations, the Review Committee recognised the necessity of an integrity function within public organisations but, given that some organisational re-arrangement of ARMS is being proposed (see Recommendation 2 above), felt that other options needed to be considered.

The management of integrity issues in research is already well-organised within UQ. The University in 2010 established the position of Research Integrity Officer within the Office of the Deputy Vice-Chancellor (Research), and developed detailed procedures for the management of research integrity allegations, in line with the Australian Code for the Responsible Conduct of Research (2007) and in conjunction with the University's Enterprise Agreement procedures for dealing with alleged misconduct/serious misconduct. Related policies were also reviewed and amended. In addition, the University's Research Ethics Office has been established for many years. Its procedures for managing research ethics in the conduct of research are robust and effective, and respected and used by researchers across the institution.

Likewise, University general policies on integrity (Sections 1.50 and 1.60 of the Policy and Procedures Library) are clear and well-known, and integrity concerns are dealt with through the audit and investigation processes, in consultation with the CMC, and through a reporting line direct to the Vice-Chancellor. The Review Committee has every expectation that this will continue in a robust fashion, and would expect that probity issues be included as a normal part of the annual internal audit plan.

Indeed to reinforce this process, the Committee recommends that the proposed Investigations Reference Group be a "clearing house" for instigating procedures to manage probity issues and allegations. Such matters would, in any case, normally come within its brief in terms of the investigation that would usually be required.

An appropriate Terms of Reference for the Group will need to be developed.

Recommendation 9

That the ARMS proposal that an Integrity Office be established within ARMS not be supported, but that the current University arrangements for overseeing integrity be maintained. The annual approved internal audit and investigation plan needs to include regular reviews of probity. In addition, probity matters should be subject to oversight by the proposed Investigations Reference Group.

CONCLUSION

The University of Queensland has much to be proud of in its ARMS Unit. However, changes to University governance and risk objectives raised a number of concerns for the Review Committee regarding the Unit's capacity to meet the University's expectations. The Unit must be in a position to respond operationally, tactically and strategically in a complex environment, where compliance responsibilities affect all parts of the institution. The review report provides an excellent opportunity for the University to consider how the key functions of audit, risk, compliance and investigations can be reorganised in order to shape the Unit's priorities and responsibilities. The Review Committee was of the view that without addressing these matters directly, the University would be inhibited from creating a Unit model that would respond effectively, add value and improve the University's operations.

Nine recommendations are provided for consideration by the Vice-Chancellor's Executive Committee. These are mapped against the ARMS Review Committee Terms of Reference items in the table below.

TERMS OF REFERENCE	REVIEW COMMITTEE RECOMMENDATIONS
1. Consistency of identified functions, scope and goals	Rec 1, Rec 7
2. UQ's and external agencies' service expectations	Rec 1, Rec 2, Rec 5
3. ARMS' efficiency and effectiveness	Rec 1, Rec 2, Rec 4, Rec 8
4. Scope of current and planned work	Rec 2, Rec 3, Rec 4, Rec 8
5. ARMS' scope, focus and service provision	Rec 2, Rec 6
6. Unit's optimum organisational structure	Rec 2, Rec 3, Rec 9
7. Current staffing profile and skill base	Rec 1, Rec 2, Rec 3
8. Systems and resources needed	Rec 1, Rec 2
9. Key performance indicators for future evaluation	Rec 1, Rec 7
10. Level of independence from management	Rec 1, Rec 2

In implementing the recommendations, the Committee's view was that the ERM and the assurance and investigations activities need to be adaptive, in moving between UQ strategic perspectives with their focus on reputational risk and innovation, to UQ operational imperatives with their attendant time-sensitive functional choices. Careful judgement by people engaged in ERM and assurance and investigations functions is also important, such as deciding when is the best time for an active or, alternatively, a preventative intervention. Future "success" for the ERM, assurance and investigations functions should be measured in terms of how "loss" or "harm" to UQ is being reduced and also, how opportunities for improvement are being assisted. A procedural approach of engaging in compliance processes for their own sake is unlikely to produce "success" for the University or its many existing and emerging stakeholders.

ACKNOWLEDGEMENTS

It has been timely to undertake a review of ARMS in accordance with the Terms of Reference. The Review Committee acknowledges the work and efforts of the staff who have contributed to the process and also thanks the Vice-Chancellor for the invitation to be involved in this review.